This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

10/661,650

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　９月１０日

出願番号
Application Number: 特願２００３－３１８４７５

[ST. 10/C]: [ＪＰ２００３－３１８４７５]

出願人
Applicant(s): 株式会社リコー

２００３年１０月　７日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３０８２７３２

【書類名】　特許願
【整理番号】　0304622
【提出日】　平成15年 9月10日
【あて先】　特許庁長官　今井　康夫　殿
【国際特許分類】　G06F 12/00　537
【発明者】
　【住所又は居所】　東京都大田区中馬込１丁目３番６号　株式会社リコー内
　【氏名】　斉藤　敦久
【発明者】
　【住所又は居所】　東京都大田区中馬込１丁目３番６号　株式会社リコー内
　【氏名】　金井　洋一
【特許出願人】
　【識別番号】　000006747
　【氏名又は名称】　株式会社リコー
【代理人】
　【識別番号】　100070150
　【弁理士】
　【氏名又は名称】　伊東　忠彦
【先の出願に基づく優先権主張】
　【出願番号】　特願2002-299714
　【出願日】　平成14年10月11日
【先の出願に基づく優先権主張】
　【出願番号】　特願2002-299721
　【出願日】　平成14年10月11日
【手数料の表示】
　【予納台帳番号】　002989
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9911477

【書類名】特許請求の範囲
【請求項１】
電子ファイルを格納する電子ファイル格納領域と、
上記電子ファイルにアクセス権限情報を付加して上記電子ファイル格納領域に格納する電子ファイル管理手段と、
上記電子ファイルへのアクセス要求に応じて、該電子ファイルを暗号化して保護した保護電子ファイルを出力する保護電子ファイル出力手段とを有することを特徴とする電子ファイル管理装置。
【請求項２】
上記電子ファイル管理手段は、
上記電子ファイルの格納要求を受けると、該電子ファイルを暗号化することによって保護された上記保護電子ファイルを取得して、該電子ファイルと該保護電子ファイルとを関連付けて上記電子ファイル格納領域に格納することを特徴とする請求項１記載の電子ファイル管理装置。
【請求項３】
上記電子ファイル管理手段は、
上記電子ファイルの格納要求を受けると、該電子ファイルを暗号化することによって保護された上記保護電子ファイルを取得して、該電子ファイルを格納する代わりに、その保護電子ファイルを上記電子ファイル格納領域に格納することを特徴とする請求項１記載の電子ファイル管理装置。
【請求項４】
上記保護電子ファイル出力手段は、
上記電子ファイルのアクセス要求を受けると、該電子ファイルを暗号化することによって保護された上記保護電子ファイルを取得して、その保護電子ファイルを出力することを特徴とする請求項１記載の電子ファイル管理装置。
【請求項５】
上記電子ファイル管理手段は、
上記電子ファイルの格納要求時に上記電子ファイルと上記保護電子ファイルとを受付けて、該電子ファイルと該保護電子ファイルとを関連付けて上記電子ファイル格納領域に格納することを特徴とする請求項１記載の電子ファイル管理装置。
【請求項６】
上記電子ファイルを暗号化する外部手段に対して、該電子ファイルと上記アクセス権限情報とを送信することによって上記保護電子ファイルを取得して、上記電子ファイル管理手段に提供する保護電子ファイル取得手段を有することを特徴とする請求項１記載の電子ファイル管理装置。
【請求項７】
上記保護電子ファイルは、上記アクセス権限情報に基づいて上記電子ファイルを暗号化されたことを特徴とする請求項１乃至６記載の電子ファイル管理装置。
【請求項８】
上記保護電子ファイル出力手段は、保護前の上記電子ファイルへのアクセス要求を受けると、保護前のドキュメントのアクセス権限があるか否かを判断し、その判断結果に基づいて、該アクセスを拒否することを特徴とする請求項１乃至６記載の電子ファイル管理装置。
【請求項９】
上記電子ファイルにアクセス権限情報を付加して電子ファイル格納領域に格納する電子ファイル管理手順と、
上記電子ファイルへのアクセス要求に応じて、該電子ファイルを暗号化して保護した保護電子ファイルを出力する保護電子ファイル出力手順とをコンピュータに実行させることを特徴とするコンピュータ実行可能なプログラム。
【請求項１０】

アクセス要求に応じて、電子ファイルをアクセス権限情報に基づいて暗号化して保護した保護電子ファイルを提供するように該電子ファイルを管理し、
上記電子ファイルに対する処理要求に応じて上記保護電子ファイルを取得し、
上記保護電子ファイルが復号できた場合、上記アクセス権限情報に従って、復号された該保護電子ファイルに対して該処理を制御することを特徴とするファイルアクセス制御方法。
【請求項１１】
上記電子ファイルを識別する電子ファイル識別情報と、上記保護電子ファイルを復号する鍵と、上記アクセス制御情報とを管理し、
上記処理要求時に、該処理要求を行ったユーザを認証するユーザ認証情報、上記電子ファイル識別情報と、該処理タイプとを取得し、
ユーザ認証が成功した場合、上記アクセス権限情報に基づいて上記処理に対する許可又は不許可を判断し、その判断結果に基づいて、上記処理への許可時に指定される処理要件と、上記鍵とを取得し、
上記鍵によって上記保護電子ファイルを復号し、
上記処理要件に従って上記処理を制御することを特徴とするファイルアクセス制御方法。

【書類名】明細書
【発明の名称】電子ファイル管理装置及びプログラム並びにファイルアクセス制御方法
【技術分野】
【０００１】
本発明は、セキュリティを必要とする技術文書などの電子ファイルを管理し、アクセス権限に応じて該電子ファイルに対するアクセス制御を行う電子ファイル管理装置及びプログラム並びにファイルアクセス制御方法に関する。
【背景技術】
【０００２】
従来より、電子ファイルを管理する電子ファイル管理装置では、格納する電子ファイルに対して予めパスワードを登録させ、ユーザからのアクセス要求を受けると、そのユーザが登録されたパスワードを入力した場合にのみ、そのパスワードに対応する電子ファイルを表示装置や外部記憶装置に出力する。
【０００３】
また、本出願人により先に出願されている（例えば、特許文献１）の「文書管理システム」は、電子化された文書を作成して登録し、承認されるとその文書を変換して印刷可能なＰＤＦと印刷不可能なＰＤＦとを作成し、利用権限に応じて閲覧できるファイルを制限するものである。
【特許文献１】特開２００１－１４２８７４号公報
【発明の開示】
【発明が解決しようとする課題】
【０００４】
しかしながら、従来の電子ファイル管理装置では、アクセス権限を認められたユーザが電子ファイルを取得した後、アクセス権限を認められていないユーザに取得した電子ファイルを渡すと、アクセス権限を認められていないユーザであってもその電子ファイルにアクセスできてしまうという問題があった。
【０００５】
また、上述した特許文献１の文書管理システムは、電子化された文書を利用権限を認められていないユーザに対しても閲覧のみを許可しつつ印刷を不可能とする好適なものであるが、利用権限を認められているユーザが印刷可能なＰＤＦを読み出した後、他の利用者にその印刷可能はＰＤＦを渡してしまうと、本来印刷可能なＰＤＦへのアクセス権限のない利用者でもＰＤＦを印刷することができてしまっていた。
【０００６】
本発明はこのような状況に鑑みてなされたものであり、オリジナルのドキュメントと、ユーザの権限に応じたアクセス制限を施した保護ドキュメントとをアクセス権限に応じて適切に管理することができる電子ファイル管理装置、方法、プログラム、及び該プログラムを記録した記録媒体を提供することである。
【課題を解決するための手段】
【０００７】
上記課題を解決するため、本発明は、請求項１に記載されるように、電子ファイルを格納する電子ファイル格納領域と、上記電子ファイルにアクセス権限情報を付加して上記電子ファイル格納領域に格納する電子ファイル管理手段と、上記電子ファイルへのアクセス要求に応じて、該電子ファイルを暗号化して保護した保護電子ファイルを出力する保護電子ファイル出力手段とを有するように構成される。
【０００８】
このような電子ファイル管理装置では、アクセス権限情報を付加して電子ファイル（ドキュメント）を管理し、保護電子ファイル（保護ドキュメント）を出力するため、オリジナルの電子ファイルに対するセキュリティを向上することができる。
【０００９】
また、本発明は、請求項２に記載されるように、上記電子ファイル管理手段は、上記電

子ファイルの格納要求を受けると、該電子ファイルを暗号化することによって保護された上記保護電子ファイルを取得して、該電子ファイルと該保護電子ファイルとを関連付けて上記電子ファイル格納領域に格納するように構成することができる。

【００１０】

また、本発明は、請求項３に記載されるように、上記電子ファイル管理手段は、上記電子ファイルの格納要求を受けると、該電子ファイルを暗号化することによって保護された上記保護電子ファイルを取得して、該電子ファイルを格納する代わりに、その保護電子ファイルを上記電子ファイル格納領域に格納するように構成することができる。

【００１１】

また、本発明は、請求項４に記載されるように、上記保護電子ファイル出力手段は、上記電子ファイルのアクセス要求を受けると、該電子ファイルを暗号化することによって保護された上記保護電子ファイルを取得して、その保護電子ファイルを出力するように構成することができる。

【００１２】

また、本発明は、請求項５に記載されるように、上記電子ファイル管理手段は、上記電子ファイルの格納要求時に上記電子ファイルと上記保護電子ファイルとを受付けて、該電子ファイルと該保護電子ファイルとを関連付けて上記電子ファイル格納領域に格納するように構成することができる。

【００１３】

また、本発明は、請求項６に記載されるように、上記電子ファイルを暗号化する外部手段に対して、該電子ファイルと上記アクセス権限情報とを送信することによって上記保護電子ファイルを取得して、上記電子ファイル管理手段に提供する保護電子ファイル取得手段を有するように構成することができる。

【００１４】

また、本発明は、請求項７に記載されるように、上記保護電子ファイルは、上記アクセス権限情報に基づいて上記電子ファイルを暗号化されるように構成することができる。

【００１５】

また、本発明は、請求項８に記載されるように、上記保護電子ファイル出力手段は、保護前の上記電子ファイルへのアクセス要求を受けると、保護前のドキュメントのアクセス権限があるか否かを判断し、その判断結果に基づいて、該アクセスを拒否するように構成することができる。

【００１６】

また、本発明は、請求項９に記載されるように、上記電子ファイルにアクセス権限情報を付加して電子ファイル格納領域に格納する電子ファイル管理手順と、上記電子ファイルへのアクセス要求に応じて、該電子ファイルを暗号化して保護した保護電子ファイルを出力する保護電子ファイル出力手順とをコンピュータに実行させるように構成することができる。

【００１７】

また、本発明は、請求項１０に記載されるように、アクセス要求に応じて、電子ファイルをアクセス権限情報に基づいて暗号化して保護した保護電子ファイルを提供するように該電子ファイルを管理し、上記電子ファイルに対する処理要求に応じて上記保護電子ファイルを取得し、上記保護電子ファイルが復号できた場合、上記アクセス権限情報に従って、復号された該保護電子ファイルに対して該処理を制御するように構成することができる。

【００１８】

また、本発明は、請求項１１に記載されるように、上記電子ファイルを識別する電子ファイル識別情報と、上記保護電子ファイルを復号する鍵と、上記アクセス制御情報とを管理し、上記処理要求時に、該処理要求を行ったユーザを認証するユーザ認証情報、上記電子ファイル識別情報と、該処理タイプとを取得し、ユーザ認証が成功した場合、上記アクセス権限情報に基づいて上記処理に対する許可又は不許可を判断し、その判断結果に基づ

いて、上記処理への許可時に指定される処理要件と、上記鍵とを取得し、上記鍵によって上記保護電子ファイルを復号し、上記処理要件に従って上記処理を制御するように構成することができる。

【発明の効果】

【００１９】

本願発明によれば、アクセス制限電子ファイルを、アクセス権限情報でアクセス権限を認められているユーザのみが復号可能であるように生成し、そのアクセス制限電子ファイルとオリジナル電子ファイルとを上記のアクセス権限情報に基づいて管理することにより、アクセス権限情報でアクセス権限を認められていないユーザに対して、アクセス制限電子ファイルをたとえ入手したとしてもアクセスできないようにすることができると共に、そのアクセス権限の管理を、管理者（アクセス権限の設定者）がアクセス権限情報を作成するだけで自動的に行うことができる。

【発明を実施するための最良の形態】

【００２０】

以下、本発明の実施の形態を図面に基づいて説明する。

【００２１】

先ず、本発明の実施形態としての電子ファイル管理装置における、各実施形態に共通する概要について説明する。

【００２２】

本発明の実施形態としての電子ファイル管理装置は、コンピュータ装置本体と、ユーザが入力を行う入力装置と、ユーザに対して各種の情報を表示する表示装置とを備えて構成される。

【００２３】

上記の入力装置は、例えばキーボードやマウスなどであり、表示装置は、例えばディスプレイなどである。

【００２４】

コンピュータ装置本体は、オリジナルのドキュメント（Document；オリジナル電子ファイル）と保護ドキュメント（Protected Document；アクセス制限電子ファイル）との管理を行い、入力装置から操作を行うユーザに認められたアクセス権限に応じて上記の表示装置に出力する。

【００２５】

コンピュータ装置本体からの出力先は上記の表示装置に限定されず、例えばプリンタをコンピュータ装置本体に接続することで、そのプリンタから印字（出力）することもできる。また、ユーザからのアクセス要求がＦＤ（フロッピー（登録商標）ディスク）などのリムーバブルディスクといった情報記録媒体への保存である場合には、その情報記録媒体に保存することとしてよい。

【００２６】

次に、本発明の第１の実施形態としての電子ファイル管理装置５０１について図１で説明する。図１は、本発明の第１の実施形態に係る電子ファイル管理装置を示す図である。

【００２７】

図１（Ａ）において、この第１の実施形態は、ドキュメント管理プログラム（Document Management Program）２１を用いてドキュメント１１（オリジナルのドキュメント；オリジナル電子ファイル）とＡＣＬ（Access Control List；アクセス権限情報）１２とを保存した際に、保護ドキュメント１３を作成して、基本的にその保護ドキュメント１３にのみアクセスさせるモデルである。

【００２８】

第１の実施形態におけるコンピュータ装置本体によって制御される電子ファイル管理装置５０１は、管理者からドキュメント１１とＡＣＬ１２とを受け取って管理するドキュメント管理プログラム（管理部）２１と、そのドキュメント１１とＡＣＬ１２とからアクセス制限をかけた保護ドキュメント１３を生成するドキュメント保護プログラム（Document

Protection Program；アクセス制限部）５１１と、電子ファイル（各種ドキュメント）やＡＣＬ１２などを格納するドキュメント管理ＤＢ（Document Management Database；格納部）２３とを有し、これらをＨＤＤなどの記憶装置（不図示）に備えてなる。

【００２９】

上記のＡＣＬ１２は、管理者によって設定されたドキュメント１１へのアクセス権限であって、アクセスしてくるユーザによってドキュメント１１へのアクセスを制限するための情報を含むものである。

【００３０】

この第１の実施形態に係る電子ファイル管理装置５０１は、物理的には、各種のプログラムやデータなどを記憶する上記した記憶装置と、ＣＰＵなどの主制御装置とを備えて構成され、この主制御装置が記憶装置に格納されたプログラムにより処理を行うことで、この電子ファイル管理装置５０１は上述した管理部と、アクセス制限部と、格納部として機能する。

【００３１】

すなわち、電子ファイル管理装置５０１は、上記の記憶部に記憶されたドキュメント管理プログラム２１により主制御装置が処理を行うことで上記した管理部として機能し、上記の記憶装置に記憶されたドキュメント保護プログラム５１１により主制御装置が処理を行うことで、上記したアクセス制限装置として機能する。

【００３２】

ＡＣＬ１２の構成例を図２に示す。この図２に示す例では、ＡＣＬ１２は、ユーザ名（User name）、アクセスタイプ（Access type）、許可情報（Permission）及び処理要件（Requirement）をパラメータとして構成される。

【００３３】

すなわち、何らかのアクセス権限を認められたユーザのユーザ名（User name）に、そのユーザに認められたアクセス権限が、ユーザからの操作命令（Access type）ごとに関連付けられて構成されている。また、ユーザによる操作命令ごとに、許可（Allowed）と拒絶（Denied）とが定められている。

【００３４】

なお、図１（Ａ）及び図１（Ｂ）、図２に示す例では、ＡＣＬ１２には処理要件（Requirement）の項が入っているが、一般的なアクセス制御しかしないのであれば、ＡＣＬ１２は処理要件（Requirement）の項がないものであってよい。

【００３５】

このＡＣＬ１２は、ドキュメント１１を作成した作成者や、電子ファイル管理装置５０１の管理者（管理者権限を持つユーザ）が作成し、そのドキュメント１１に付与しておくこととする。電子ファイル管理装置５０１は、ドキュメント管理プログラム２１により、入力装置によるユーザからの各操作命令に対し、このＡＣＬ１２に基づいて、上述した各種の出力を行う。

【００３６】

次に、第１の実施形態にかかる電子ファイル管理装置５０１における電子ファイルの格納時の動作について、図１（Ａ）、図３、図４、図５を参照して説明する。

【００３７】

ドキュメント管理プログラム２１がドキュメント１１とＡＣＬ１２とを受け取って保存する際、ドキュメント管理プログラム２１は受け取ったドキュメント１１とＡＣＬ１２をドキュメント保護プログラム５１１に渡して保護ドキュメント１３を受け取る。

【００３８】

すなわち、ドキュメント保護プログラム５１１は、受け取ったＡＣＬ１２に設定されているアクセス権限の制限と同一の制限がドキュメント１１にかけられるように、ドキュメント１１から保護ドキュメント１３を生成する。

【００３９】

このドキュメント保護プログラム５１１による保護ドキュメント１３の生成（暗号化）

とその復号化にかかるドキュメント保護・印刷システムの構成例を図３に示す。以下の説明では、この保護ドキュメント１３の活用（復号化）用途を、プリンタ５０３により記録紙に印刷することであるとする。

【００４０】

この図３に示すドキュメント保護・印刷システム５００１は、電子ファイル管理装置５０１、印刷用端末５０２、プリンタ５０３及びアクセスコントロールサーバ５０４を有する。

【００４１】

電子ファイル管理装置５０１と印刷用端末５０２は、表示装置（例えば、ＬＣＤ）、入力装置（例えば、キーボード）、外部記録装置（例えば、ＦＤＤ、ＨＤＤ）などを備えたコンピュータ端末を適用できる。なお、電子ファイル管理装置５０１にはドキュメント保護プログラム５１１が、印刷用端末５０２にはドキュメント印刷プログラム５２１がそれぞれ実装されている。

【００４２】

ドキュメント保護プログラム５１１は、ドキュメントファイルに電子ファイル管理装置５０１の管理者としてのユーザの入力操作に応じた印刷要件を設定するとともに、暗号化アルゴリズム（ＲＣ４、Ｔｒｉｐｌｅ　ＤＥＳ、ＩＤＥＡなど）を用いてドキュメントファイルを暗号化し、保護ドキュメントを生成する処理を行うプログラムである。

【００４３】

なお、管理者の入力操作に応じてドキュメント保護プログラム１１１がドキュメントファイルに設定する印刷要件の例としては、地紋印刷（Background Dot Pattern：以下、ＢＤＰという）、機密印刷（Private Access：以下、ＰＡＣという）、電子透かし（Digital Watermark：以下、ＤＷＭという）の付加、バーコード付加（Embedding Barcode：以下、ＥＢＣという）、機密ラベルスタンプ（Security Label Stamp：以下、ＳＬＳという）などが挙げられる。

【００４４】

ドキュメント印刷プログラム５２１は、ユーザの入力操作に応じ、保護ドキュメント１３を復号化するとともに、設定されている印刷要件に応じた印刷処理をプリンタ５０３に実行させる処理を行うプログラムである。

【００４５】

アクセスコントロールサーバ５０４は、ユーザがドキュメントを印刷しようとする場合に、ドキュメント印刷プログラム５２１からの要求に応じてＡＣＬ１２を参照し、ドキュメントを印刷する権限があるか否か、印刷要件がどのように設定されているかを取得するサーバである。

【００４６】

アクセスコントロールサーバ５０４には、ユーザ各人の認証用の情報（ユーザ名とパスワードとの組）が格納されたユーザデータベース５４１と、ユーザ各人ごとに設定された印刷要件を含むＡＣＬ１２が登録されるＡＣＬデータベース５４２とが接続されている。

【００４７】

上述のドキュメント保護・印刷システム５００１において、ドキュメント１１とＡＣＬ１２とを取得したドキュメント保護プログラム５１１は、上記の保護ドキュメント１３を生成するに当たって、ドキュメントファイルごとに固有のドキュメントＩＤ（Document ID）を生成し、復号に使用する暗号鍵（Key）とＡＣＬ１２とをこれに関連づけてアクセスコントロールサーバ５０４へ送信し、登録する。

【００４８】

また、ドキュメント保護プログラム５１１は、図５に示すように、暗号鍵を用いてドキュメント１１を暗号化し、その暗号化されたドキュメントファイル（暗号化ドキュメント）に対してドキュメントＩＤを付加して保護ドキュメント１３を生成する。

【００４９】

こうして保護ドキュメント１３が生成されると、ドキュメント管理プログラム２１は、

受け取った保護ドキュメント１３をドキュメント１１及びＡＣＬ１２と共に（関連づけて）ドキュメント管理ＤＢ２３に格納する。こうして、電子ファイル管理装置５０１は、ドキュメント１１と保護ドキュメント１３のペア（これをドキュメント・ペア（Ｄｏｃｕｍｅｎｔ　Ｐａｉｒ）と呼ぶ）にＡＣＬ１２を付与して（関連付けて）管理する。

【００５０】

次に、第１の実施形態にかかる電子ファイル管理装置５０１が、管理しているドキュメント・ペアに対してユーザからアクセス要求を受けた時の動作について、図１（Ｂ）、図３を参照して説明する。

【００５１】

ドキュメント管理プログラム２１は、ユーザからドキュメント・ペアに対するアクセス要求を受けるとユーザの認証を行う。この認証では、ドキュメント管理プログラム２１は、ドキュメント・ペアに付与されているＡＣＬ１２を参照して、アクセスしてきたユーザに参照権限がある、すなわちｒｅａｄ権限があると判断すると、保護ドキュメント１３を返す。すなわち、電子ファイル管理装置５０１から上述のように表示装置などに出力する。

【００５２】

上記の認証で、アクセスしてきたユーザに参照権限がない、すなわちｒｅａｄ権限が認められていないとドキュメント管理プログラム２１が判断すると、表示装置にその旨を表示する。

【００５３】

この出力された保護ドキュメント１３の復号化について、上述した図３に示すドキュメント保護・印刷システム５００１の例により説明する。

【００５４】

なお、図３に示すドキュメント保護・印刷システム５００１の例では、ドキュメントファイルを印刷や参照しようとするユーザに対する上述の電子ファイル管理装置５０１からの出力として、管理者によりＦＤなどの情報記録媒体による受け渡しを行う場合と、通信網により印刷用端末５０２へ送信する場合とを示している。

【００５５】

ユーザがドキュメント１１を印刷しようとする場合には、印刷用端末５０２に保護ドキュメント１３を実装する。例えば、上述のように電子ファイル管理装置５０１から情報記録媒体に出力（記録）された保護ドキュメント１３を外部記録装置を用いて印刷用端末５０２に読み取らせても良いし、印刷用端末５０２が電子ファイル管理装置５０１と通信可能である場合には、通信網を介して電子ファイル管理装置５０１から保護ドキュメント１３を印刷用端末５０２に出力させるようにしてもよい。

【００５６】

ユーザが、印刷用端末５０２の入力装置を介してドキュメント印刷プログラム５２１に対して印刷を指示すると、印刷を要求されたドキュメント印刷プログラム５２１は、ユーザを認証するために必要となるユーザ名とパスワードの入力をユーザに要求する。例えば、ドキュメント印刷プログラム５２１は、印刷用端末５０２の表示装置にメッセージを表示するなどして、ユーザ名とパスワードの入力を要求する。

【００５７】

ドキュメント印刷プログラム５２１は、ユーザから入力されたユーザ名とパスワードとをアクセスコントロールサーバ５０４へ送信して、ユーザ認証を要求する。

【００５８】

アクセスコントロールサーバ５０４は、ドキュメント印刷プログラム５２１から受け渡されたユーザ名とパスワードとを用いてユーザ認証を行い、ユーザを特定する。

【００５９】

ユーザを特定すると、アクセスコントロールサーバ５０４は、ＡＣＬデータベース５４２を参照し、ドキュメントファイルを印刷する権限がユーザにあるか否かや、ユーザがドキュメントファイルを印刷する際には、どのような印刷要件が設定されているかといった

、アクセス権限の制限の情報を取得する。

【００６０】

ユーザにドキュメントファイル（保護ドキュメント１３）を印刷する権限がある場合、アクセスコントロールサーバ５０４は、その旨を示す認証情報とともに、保護ドキュメント１３を復号化するための暗号鍵とユーザがドキュメントファイルを印刷する際の印刷要件とを印刷用端末５０２を介してドキュメント印刷プログラム５２１に通知する。

【００６１】

アクセスコントロールサーバ５０４から認証情報とともに、暗証鍵と印刷要件とを取得したドキュメント印刷プログラム５２１は、暗号鍵を用いて保護ドキュメント１３を復号化してドキュメント１１に復元する。

【００６２】

そしてドキュメント印刷プログラム５２１は、印刷要件を満たすようにプリンタ５０３に印刷処理を実行させる。例えば、ドキュメントファイルにＢＤＰ（地紋印刷）が印刷要件として設定されている場合には、ドキュメントの内容とともに地紋を印刷する。

【００６３】

以上により、ドキュメントファイルを印刷する際に、管理者がユーザ各人に対して設定した印刷要件、すなわちＡＣＬ１２としてユーザ各人に対して設定したアクセス権限の制限を強制することが可能となる。

【００６４】

次に、第１の実施形態に係るドキュメント管理プログラム２１によって実現される機能構成について図４で説明する。図４は、第１の実施形態に係るドキュメント管理プログラムによって実現される機能構成を示す図である。図中、クライアントｃ１及びｃ２は、同一クライアントであってもよい。

【００６５】

図４において、ドキュメント管理プログラム２１によって、少なくとも、ドキュメント保管要求受付部２１ａと、ドキュメント保管部２１ｂ保護ドキュメント取得部２１ｃと、ドキュメント参照要求受付部２１ｄと、ドキュメント取得部２１ｅとが機能として構成される。

【００６６】

ドキュメント保管要求受付部２１ａは，ドキュメント１１の保管を要求するクライアントｃ１から，ドキュメント保管要求とともにドキュメント１１とＡＣＬ１２を受け取ると，受け取ったドキュメント１１とＡＣＬ１２をドキュメント保管部２１ｂに渡す。

【００６７】

ドキュメント保管部２１ｂは受け取ったドキュメント１１をドキュメント管理ＤＢ２３に格納し、受け取ったＡＣＬ１２をその格納したドキュメント１１のＡＣＬ１２として設定する。ドキュメント保管部２１ｂは格納したドキュメント１１の識別子（ドキュメントＩＤ）を返す。

【００６８】

ドキュメント保管要求受付部２１ａは、ドキュメント保管部２１ｂからドキュメントＩＤを受け取ると、ドキュメント１１、ＡＣＬ１２、ドキュメントＩＤを保護ドキュメント取得部２１ｃに渡す．保護ドキュメント取得部２１ｃはドキュメント１１とＡＣＬ１２をドキュメント保護プログラム５１１に渡して保護ドキュメント１３を取得し、ドキュメントＩＤと保護ドキュメント１３をドキュメント保管部２１ｂに渡す。

【００６９】

ドキュメント保管部２１ｂはドキュメントＩＤで指定されたドキュメント１１に関連付けてその保護ドキュメント１３をドキュメント管理ＤＢ２３に格納する。

【００７０】

ドキュメント保管要求受付部２１ａは、ドキュメント保管要求をしたクライアントｃ１にドキュメントＩＤを返す。返すタイミングは、ドキュメント１１を保管してすぐでも良いし、保護ドキュメント１３が格納されたことを確認した後でも良い。

【００７１】
また、ドキュメント参照要求受付部２１ｄは、ドキュメント１１の参照を要求するクライアントｃ２から、ドキュメント参照要求とともにドキュメントＩＤを受け取ると、受け取ったドキュメントＩＤをドキュメント取得部２１ｅに渡す。
【００７２】
ドキュメント取得部２１ｅは、受け取ったドキュメントＩＤをもとにドキュメント管理ＤＢ２３から該当するドキュメント１１のＡＣＬ１２を確認し、参照権限のあるユーザからの要求であれば、そのドキュメント１１とともに格納されている保護ドキュメント１３をドキュメント管理ＤＢ２３から取得し、ドキュメント参照要求受付部２１ｄに返す。
【００７３】
ドキュメント参照要求受付部２１ｄは、ドキュメント参照要求をしたクライアントｃ２に受け取った保護ドキュメント１３を返す。ドキュメント参照要求をしてクライアントｃ２を使用しているユーザに参照権限がない場合にはエラーを返す。その一方で、ユーザにオリジナルを参照する特別な権限が与えられている場合には、保護ドキュメント１３を返すのではなく、オリジナルのドキュメント１１を返すようにしても良い。
【００７４】
次に、ドキュメント１１から保護ドキュメント１３を生成する際のドキュメント保護プログラム５１１及びアクセスコントロールサーバ５０４の動作、及び保護ドキュメント１３をドキュメント１１に復元して印刷する際のドキュメント印刷プログラム５２１及びアクセスコントロールサーバ５０４の動作についてさらに詳しく説明する。
【００７５】
ドキュメント保護プログラム５１１が保護ドキュメント１３を生成する際の動作を図で説明する。図５は、ドキュメント保護プログラムの動作を示す図である。
【００７６】
図５において、ドキュメント保護プログラム５１１は、電子ファイル管理装置５０１の入力装置における管理者の入力操作によってドキュメントファイルとＡＣＬ１２とを取得すると、ドキュメントファイルの暗号化・復号化するための暗号鍵を生成する。そして、ドキュメント保護プログラム５１１は、生成した暗号鍵を用いてドキュメントファイルを暗号化して、暗号化ドキュメントを生成する。
【００７７】
さらにドキュメント保護プログラム５１１は、ドキュメントファイルごとに固有のドキュメントＩＤを暗号化ドキュメントに添付して保護ドキュメント１３を生成する。
【００７８】
保護ドキュメント１３を生成した後、ドキュメント保護プログラム５１１は電子ファイル管理装置５０１の通信機能を用いて、暗号鍵とＡＣＬ１２とドキュメントＩＤとをアクセスコントロールサーバ５０４へ送信し、これらの登録をアクセスコントロールサーバ５０４に要求する。
【００７９】
暗号鍵とＡＣＬ１２とドキュメントＩＤとをドキュメント保護プログラム５１１から受け渡されたアクセスコントロールサーバ５０４は、図６に示すように、これらを関連づけて一つのレコードとしてＡＣＬデータベース５４２に記録保持する。図６は、ＡＣＬデータベースに記録される情報の構造例を示す図である。図６において、ＡＣＬデータベース５４２は、ドキュメントＩＤ（Document ID）ごとに、暗号鍵（Key）と、ＡＣＬ１２とを管理する。
【００８０】
なお、上記の例においてはドキュメントＩＤの生成や暗号鍵の生成をドキュメント保護プログラム５１１が行う場合を示したが、これらの処理はアクセスコントロールサーバ５０４やドキュメントＩＤの生成や暗号鍵の生成を行う別のサーバ（不図示）などで行っても良い。
【００８１】

また、電子ファイル管理装置５０１とアクセスコントロールサーバ５０４との間が専用回線ではなくネットワーク網を介して接続されており、暗号鍵など送信する際に盗聴される懸念がある場合には、ＳＳＬ（Secure Socket Layer）を用いて通信を行えばよい。

【００８２】

ドキュメント保護プログラム５１１がアクセスコントロールサーバ５０３と通信する際のプロトコルは、どのようなものを用いてもよい。例えば、分散オブジェクト環境を導入し、Ｊａｖａ（登録商標）　ＲＭＩ（Remote Method Invocation）やＳＯＡＰ（Simple Object Access Protocol）をベースとして情報を送受信するようにしても良い。その場合、アクセスコントロールサーバ５０４は、例えばregister (String docId, byte[] key, byte[] acl)のようなメソッドを実装するようにしてもよい。ＳＯＡＰであれば、ＨＴＴＰＳの上でＳＯＡＰプロトコルをやりとりし、ＲＭＩであればＳＳＬベースのSocketFactoryを用いてＲＭＩを実行するようにすれば、ネットワーク上でのセキュリティを確保できる。

【００８３】

次に、ドキュメント印刷プログラム５２１が保護ドキュメント１３を印刷する際の動作について図７で説明する。

【００８４】

図７は、ドキュメント印刷プログラム及びアクセスコントロールサーバの動作の流れを示す図である。

【００８５】

図７において、ドキュメント印刷プログラム５２１は、印刷用端末５０２の入力装置におけるユーザの入力操作によって保護ドキュメント１３とユーザ名とパスワードとを取得すると、保護ドキュメント１３に添付されているドキュメントＩＤを取得する（ステップＳ５１１）。

【００８６】

そして、ユーザ名とパスワードとドキュメントＩＤとアクセスタイプ（ユーザが要求する処理を示す情報。ここでは、保護ドキュメント１３を印刷しようとするので“print”となる。）とをアクセスコントロールサーバ５０４へ送信して、アクセス権限があるか否かのチェックを要求する（ステップＳ５１２）。

【００８７】

なお、図８は、アクセスコントロールへのＳＯＡＰによる問い合わせの例を示す図であり、ユーザ名（userId）とドキュメントＩＤ（docId）とアクセスタイプ（accessType）とを渡してアクセスが許可されているかを問い合わせるＳＯＡＰメッセージ（isAllowed）を送付し、その結果（isAllowedResponse）を受け取っている例である。結果には、許可されているということ（allowedがtrue）と要件（requirements）とが含まれている。

【００８８】

アクセスコントロールサーバ５０４は、ドキュメント印刷プログラム５２１からユーザ名とパスワードとドキュメントＩＤとアクセスタイプとを取得すると、ユーザデータベース５４１に登録されている情報を参照し（ステップＳ５１３）、ユーザ認証を行う（ステップＳ５１４）。

【００８９】

換言すると、アクセスコントロールサーバ５０４は、ユーザデータベース５４１に登録されている情報を参照し、ドキュメント印刷プログラム５２１から取得した情報に含まれるユーザ名とパスワードとを組としたものが、ユーザデータベース５４１に組として登録されているか否かを判断する。

【００９０】

ユーザ認証に失敗した場合（換言すると、ドキュメント印刷プログラム５２１から受け渡された情報に含まれるユーザ名とパスワードとを組としたものがユーザデータベース５４１に登録されていない場合）、アクセスコントロールサーバ５０４は、許可情報（ユーザが要求する処理を許可するか否かを示す情報）を「不許可」として印刷用端末５０２へ

送信し、ドキュメント印刷プログラム５２１へ受け渡す（ステップＳ５１５）。なお、この場合は「エラー」とした許可情報をドキュメント印刷プログラム５２１へ受け渡すようにしてもよい（ステップＳ５１６）。

【００９１】

一方、ユーザ認証に成功した場合、アクセスコントロールサーバ５０４は、ＡＣＬデータベース５４２に格納されているレコードのうち、ドキュメント印刷プログラム５２１から取得した情報に含まれるドキュメントＩＤに関するレコードを読み出す（ステップＳ５１７）。

【００９２】

アクセスコントロールサーバ５０４は、読み出したレコードに含まれるＡＣＬ１２を取得し、ドキュメント印刷プログラム５２１から取得したユーザ名及びアクセスタイプに基づいて、ＡＣＬ１２から許可情報および印刷要件を取得する（ステップＳ５１８）。

【００９３】

換言すると、アクセスコントロールサーバ５０４は、ユーザ名とアクセスタイプとに基づいて、予めＡＣＬ１２に設定されている許可情報と印刷要件とを取得する（ステップＳ５１９）。

【００９４】

ＡＣＬ１２から取得した許可情報が「許可」を示すか否かを判断する（ステップＳ５２０）。ＡＣＬ１２から取得した許可情報が「許可」である場合、アクセスコントロールサーバ５０４は、レコードに格納されている暗号鍵と印刷要件とを許可情報とともに印刷用端末５０２へ送信してドキュメント印刷プログラム５２１に受け渡す（ステップＳ５２１）。

【００９５】

一方、ＡＣＬ１２から取得した許可情報が「不許可」である場合、アクセスコントロールサーバ５０４は、許可情報のみを印刷用端末５０２へ送信してドキュメント印刷プログラム５２１に受け渡す。

【００９６】

アクセスコントロールサーバ５０４から許可情報を受け渡されたドキュメント印刷プログラム５２１は、取得した許可情報を参照し、「不許可」である場合には、印刷用端末５０２の表示装置にメッセージを表示するなどして、要求された処理を実行できないことをユーザに通知する（ステップＳ５２２）。

【００９７】

一方、取得した許可情報が「許可」である場合には、許可情報と共に受け渡された暗号鍵を用いて、保護ドキュメントのうちの暗号化ドキュメントの部分を復号してドキュメントファイルに復元する（ステップＳ５２３）。

【００９８】

また、ドキュメント印刷プログラム５２１は、許可情報と共に取得した印刷要件を満足するようにプリンタドライバを設定し（例えば、ＰＡＣが指定されていれば機密印刷モードに設定する）、プリンタ５０３にドキュメントの印刷処理を実行させる。

【００９９】

なお、必要があれば、印刷用端末５０２の表示装置にメッセージを表示するなどして、印刷パラメータの設定をユーザに要求するようにしてもよい。

【０１００】

アクセスコントロールサーバ５０４から取得した印刷要件を満足する印刷をプリンタ５０３では実行できない場合、換言すると、プリンタ５０３がＡＣＬ１２に設定されていた印刷要件を満たす機能を備えていない場合には、その旨を示すメッセージを表示装置に表示させるなどしてユーザに通知し、印刷は行わずに処理を終了する。

【０１０１】

以上の動作によって、ユーザごとに異なるアクセス権や印刷要件を設定することが可能となる。また、上記のように、アクセスコントロールサーバ５０４側でドキュメントファ

イルに対するアクセス権限を判断するシステム構成においては、ＡＣＬデータベース５４２に登録されているＡＣＬ１２の内容を電子ファイル管理装置５０１やアクセスコントロールサーバ５０４における入力操作によって変更できるようにてもよく、この場合には、保護ドキュメント１３を配布した後で印刷要件を変更したりすることが可能となる。

【０１０２】

例えば、既に配布した保護ドキュメント１３に対するアクセス権限を新たなユーザに設定したり、特定のユーザに対して印刷要件を追加することなどが可能となる。

【０１０３】

なお、本実施形態を用いる図３に示すドキュメント保護・印刷システム５００１が上記のような手法でドキュメントファイルを保護していることを知っている者は、ドキュメント印刷プログラム５２１に成りすますプログラムをコンピュータ端末に実行させて暗号鍵を不正に入手し、保護ドキュメント１３を復号することも可能ではある。この場合は、ＡＣＬ１２として設定されている印刷要件を強制されることなく、保護ドキュメント１３を印刷できてしまうこととなる。

【０１０４】

このため、単に暗号鍵のみを用いてドキュメントファイルを暗号化するのではなく、ドキュメント保護プログラム５１１の内部に埋め込まれた秘密鍵と暗号鍵とを合わせたもの（排他的論理和を取ったもの）でドキュメントファイルを暗号化することが好ましい。

【０１０５】

この場合は、ドキュメント印刷プログラム５２１にも同一の秘密鍵を埋め込んでおくことで、管理者が設定した印刷要件を印刷時に強制するドキュメント印刷プログラム５２１のみが、保護ドキュメント１３を復号して印刷することが可能となる。

【０１０６】

また、図３を用いて上述したドキュメント保護・印刷システム５００１においては、ドキュメント印刷プログラム５２１は、ドキュメントファイルの印刷に関する処理のみを行っているが、ドキュメント印刷プログラム５２１は、ドキュメントファイルの内容をユーザに提示したり、ドキュメントファイルを編集する機能を備えていても良い。例えば、Adobe Acrobat（登録商標）のプラグインとしてこの機能を実現することが可能である。

【０１０７】

なお、この第１の実施形態としての電子ファイル管理装置５０１では、上述した図２に示すＡＣＬ１２の例には記載していないが、ＡＣＬ１２のＡｃｃｅｓｓ　ｔｙｐｅとして例えばＧｅｔＯｒｉｇｉｎａｌ（オリジナル電子ファイルへのアクセス権限）を定義し、そのＧｅｔＯｒｉｇｉｎａｌのアクセス権限を認められているユーザがドキュメント・ペアにアクセスした場合には、ドキュメント管理プログラム５１１は保護ドキュメント１３を返すのではなく、ドキュメント１１を返すようにしてもよい。

【０１０８】

すなわち、電子ファイル管理装置５０１がＧｅｔＯｒｉｇｉｎａｌを定義されたＡＣＬ１２に基づいてユーザ認証を行い、アクセスしたユーザにＧｅｔＯｒｉｇｉｎａｌのアクセス権限が認められている場合にはドキュメント１１を電子ファイル管理装置５０１から上述のように出力するようにしてもよい。

【０１０９】

また、ＡＣＬ１２にオリジナル電子ファイルであるドキュメント１１へのアクセス権限を定義しなくても、特別なユーザのみ（例えば保存したユーザのみ）がドキュメント１１へのアクセス権限を認められることとしてもよい。すなわち、ドキュメント管理プログラム５１１が、予め設定された特別なユーザのみにドキュメント１１へのアクセス権限を認めることとしてもよい。

【０１１０】

本実施形態によれば、ドキュメント管理プログラム５１１により管理・格納されているドキュメントに対するアクセス制御（アクセス権限の制限）と、ユーザに渡された（電子ファイル管理装置５０１から出力された）ドキュメント（ポータブルドキュメント）への

アクセス制御とを統一することができる。

【０１１１】

また、管理者はＡＣＬ１２としてアクセス権限の制限を設定し、ドキュメント１１とＡＣＬ１２とをドキュメント管理プログラム５１１に渡すよう電子ファイル管理装置５０１を入力装置により操作するだけで、設定したアクセス権限に応じて保護ドキュメント１３をユーザに渡すよう電子ファイル管理装置５０１に管理させることができる。

【０１１２】

すなわち、管理者がＡＣＬ１２としてアクセス権限の制限を一度設定するだけで、電子ファイル管理装置５０１は、表示装置や外部記録装置などへの出力をそのアクセス権限の制限により管理することができる。

【０１１３】

さらに、上述のようにオリジナル電子ファイルへのアクセス権限を定義することで、電子ファイル管理装置５０１は、上記したアクセス権限の制限による管理をドキュメント１１と保護ドキュメント１３とに対して行うことができる。すなわち、電子ファイル管理装置５０１は、ＡＣＬ１２として設定されたアクセス権限に応じてドキュメント１１又は／及び保護ドキュメント１３を出力するよう管理することができる。

【０１１４】

図１（Ａ）及び図１（Ｂ）に示す電子ファイル管理装置５０１の他の例を図９で説明する。図９は、本発明の第１の実施形態に係る電子ファイル管理装置の他の例を示す図である。図１（Ａ）及び図１（Ｂ）に示す電子ファイル管理装置５０１において、図９（Ａ）及び図９（Ｂ）に示すようにオリジナルのドキュメント１１－２のみを管理することもできる。

【０１１５】

図９（Ａ）において、ドキュメント管理プログラム２１がドキュメント１１－２のみを受け取って保存する際、ドキュメント管理プログラム２１は、受け取ったドキュメント１１－２を、直接ドキュメント管理ＤＢ２３に格納する。また、図９（Ｂ）において、ドキュメント管理プログラム２１は、ユーザからのドキュメント・ペアに対してではなく、ドキュメント１１－２に対するアクセス要求に対してドキュメント１１－２を表示装置などに出力する。この場合、ユーザの認証を行っても良いが、ＡＣＬ１２との比較によるユーザのｒｅａｄ権限の判断は行わない。

【０１１６】

次に、本発明の第２の実施形態としての電子ファイル管理装置５０５について、図１０を参照して説明する。図１０は、本発明の第２の実施形態に係る電子ファイル管理装置を示す図である。

【０１１７】

この第２の実施形態は、ドキュメント管理プログラム２１が、第１の実施形態でドキュメント管理ＤＢ２３にドキュメント１１と保護ドキュメント１３（ドキュメント・ペア）をＡＣＬ１２に関連付けて格納していたのに替えて、保護ドキュメント１３を格納し、ドキュメント１１を破棄するものである。

【０１１８】

すなわち、第１の実施形態のようにドキュメント１１を残しておくと、そのドキュメント１１にアクセス可能なユーザがプロテクトされていないドキュメント１１を流通させてしまう可能性がある。そのようなことが心配される環境では、この第２の実施形態とすることで保護ドキュメント１３を好適に管理することができる。

【０１１９】

この第２の実施形態の電子ファイル管理装置５０５は、物理的な構成は上述した第１の実施形態と同様であり、図１０に示すように、ドキュメント管理プログラム５１と、ドキュメント保護プログラム２２と、ドキュメント管理ＤＢ２３と、をＨＤＤなどの記憶部（不図示）に備えてなる。

【０１２０】

上述した第１の実施形態と同様のものについては同じ符号とし、説明を省略する。

【０１２１】

また、ドキュメント保護プログラム２２がドキュメント１１から保護ドキュメント１３を生成する動作や、ユーザからのアクセスにより出力された保護ドキュメント１３を復号してプリンタにより印刷する際のシステムや動作も、図３、図５から図８を用いて上述したものと同様であってよい。

【０１２２】

この第２の実施形態にかかる電子ファイル管理装置５０５における電子ファイル格納時の動作について、図１０（Ａ）を参照して説明する。

【０１２３】

ドキュメント管理プログラム５１にドキュメント１１とＡＣＬ１２を渡し、ユーザが入力装置から格納するよう操作すると、ドキュメント管理プログラム５１は、受け取ったドキュメント１１とＡＣＬ１２とをドキュメント保護プログラム５１１に渡して保護ドキュメント１３を受け取る。すなわち、上述のようにドキュメント保護プログラム５１１に保護ドキュメント１３を生成させる。

【０１２４】

生成された保護ドキュメント１３を受け取ると、ドキュメント管理プログラム５１は、受け取った保護ドキュメント１３をドキュメント管理ＤＢ２３に格納し、ドキュメント１１とＡＣＬ１２とは破棄する。

【０１２５】

この第２の実施形態にかかる電子ファイル管理装置５０５が、管理しているドキュメントに対してユーザからアクセス要求を受けた時の動作について、図１０（Ｂ）を参照して説明する。

【０１２６】

ドキュメント管理プログラム５１はドキュメントに対するアクセス要求を受けると、ドキュメント管理ＤＢ２３に格納している保護ドキュメント１３を返す。すなわち、電子ファイル管理装置５０５から上述のように表示装置などに出力する。

【０１２７】

本実施形態では、ドキュメント１１は破棄され、保護ドキュメント１３はユーザによって読み出された後、ＡＣＬ１２に従ってアクセス制御されるため、ドキュメント管理プログラム５１でアクセス制御を行う必要はない。

【０１２８】

しかし、保護ドキュメント１３を取得されると暗号を解読されて内容にアクセスされる可能性もあるため、その可能性を少しでも減らすために、上述した第１の実施形態と同様に、ドキュメント管理プログラム５１が保護ドキュメント１３をドキュメント管理ＤＢ２３に格納する際、保護ドキュメント１３にＡＣＬ１２を関連付けて格納（ＡＣＬ１２を付与して管理）し、そのＡＣＬ１２に基づいてアクセス制御を行うようにしてもよい。すなわち、上記したドキュメント１１を破棄する際に、ドキュメント管理プログラム５１はＡＣＬ１２を破棄せず、保護ドキュメント１３に関連付けてドキュメント管理ＤＢ２３に格納することとしてもよい。

【０１２９】

このようにアクセス制御を行うことで、ドキュメント管理プログラム５１により管理・格納されているドキュメントに対するアクセス制御（アクセス権限の制限）と、ユーザに渡された（電子ファイル管理装置５０５から出力された）ドキュメント（ポータブルドキュメント）へのアクセス制御とを統一することができる。

【０１３０】

本実施形態によれば、暗号化されていないドキュメント１１を破棄することにより、管理しているドキュメントをより確実に保護することができる。

【０１３１】

図１０（Ａ）及び図１０（Ｂ）に示す電子ファイル管理装置５０５の他の例を図１１で

説明する。図１１は、本発明の第２の実施形態に係る電子ファイル管理装置の他の例を示す図である。図１０（Ａ）及び図１０（Ｂ）に示す電子ファイル管理装置５０５－２において、図１１（Ａ）及び図１１（Ｂ）に示すようにオリジナルのドキュメント１１－２のみを管理することもできる。

【０１３２】

図１１（Ａ）において、ドキュメント管理プログラム５１がドキュメント１１－２のみを受け取って保存する際、ドキュメント管理プログラム５１は、受け取ったドキュメント１１－２を、直接ドキュメント管理ＤＢ２３に格納する。また、図１１（Ｂ）において、ドキュメント管理プログラム５１は、ユーザからのドキュメント・ペアに対してではなく、ドキュメント１１－２に対するアクセス要求に対してドキュメント１１－２を表示装置などに出力する。

【０１３３】

次に、第２の実施形態に係るドキュメント管理プログラム５１によって実現される機能構成について図１２で説明する。図１２は、第２の実施形態に係るドキュメント管理プログラムによって実現される機能構成を示す図である。

【０１３４】

図１２において、図４に示すドキュメント管理プログラム２１とは異なり、こちらはオリジナルのドキュメント１１はドキュメント管理ＤＢ１３で管理しない実施例である。ドキュメント管理プログラム５１によって、少なくとも、ドキュメント保管要求受付部５１ａと、ドキュメント保管部５１ｂと、保護ドキュメント取得部５１ｃと、ドキュメント参照要求受付部５１ｄと、ドキュメント取得部５１ｅとが機能として構成される。

【０１３５】

ドキュメント保管要求受付部５１ａは、ドキュメント保管部５１ｂにドキュメント１１を渡さず、ＡＣＬ１２のみを渡してドキュメントＩＤを取得しておく。図１２に示すドキュメント管理プログラム５１では、ＡＣＬ１２のみが設定された空のドキュメントエリア１３－２をドキュメント管理ＤＢ２３に作成しておいて、後からその空のドキュメントエリア１３－２に保護ドキュメント１３を格納する例を示している。

【０１３６】

保護ドキュメント取得部５１ｃと、ドキュメント参照要求受付部５１ｄと、ドキュメント取得部５１ｅとは、図４に示す保護ドキュメント取得部２１ｃと、ドキュメント参照要求受付部２１ｄと、ドキュメント取得部２１ｅと同様の動作を行うため、その説明を省略する。

【０１３７】

もちろん、空のドキュメントエリア１３－２を先に作らず、保護ドキュメント１３を作成してからドキュメントエリア１３－２を確保して格納するようにしても良い。

【０１３８】

この例の場合、ドキュメント管理プログラム５１は保護ドキュメント１３のみを管理するプログラムとなるため、ドキュメント保護プログラム５１１と同じコンピュータで稼動させるのが現実的である。

【０１３９】

次に、本発明の第３の実施形態としての電子ファイル管理装置６１について、図１３で説明する。

【０１４０】

この第３の実施形態は、ドキュメント管理プログラムが、第１の実施形態でドキュメント保護プログラム５１１に保護ドキュメント１３を生成させて、ドキュメント管理ＤＢ２３にドキュメント１１と保護ドキュメント１３（ドキュメント・ペア）をＡＣＬ１２に関連付けて格納していたのに替えて、ドキュメント１１をＡＣＬ１２に関連付けてそのまま格納し、ユーザからアクセス要求を受けた際にドキュメント保護プログラム５１１に保護ドキュメント１３を生成させて上述のように出力するものである。

【０１４１】

すなわち、第１の実施形態のような管理を行う場合、保護ドキュメント１３を保存しておく分だけディスク領域を多く必要とすることになる。そこで、この第３の実施形態は、ドキュメントへのアクセスがユーザから要求されたときに動的に保護ドキュメント１３を作成することで、余分なディスク領域を使用せずにすむ好適な管理を行うことができる。

【０１４２】

図１３は、第３の実施形態の電子ファイル管理装置の例を示す図である。図１３において、この第３の実施形態の電子ファイル管理装置５０６は、物理的な構成は上述した第１の実施形態と同様であり、ドキュメント管理プログラム６１と、ドキュメント保護プログラム５１１と、ドキュメント管理ＤＢ２３と、をＨＤＤなどの記憶部（不図示）に備えてなる。上述した第１の実施形態と同様のものについては同じ符号とし、説明を省略する。

【０１４３】

また、ドキュメント保護プログラム５１１がドキュメント１１から保護ドキュメント１３を生成する動作や、ユーザからのアクセスにより出力された保護ドキュメント１３を復号してプリンタ５０３により印刷する際のシステムや動作も、図３、図５から図８を用いて上述したものと同様であってよい。

【０１４４】

この第３の実施形態にかかる電子ファイル管理装置５０６における電子ファイル格納時の動作について、図１３（Ａ）を参照して説明する。

【０１４５】

ドキュメント管理プログラム６１にドキュメント１１とＡＣＬ１２を渡し、ユーザが入力装置から格納するよう操作すると、ドキュメント管理プログラム６１は、受け取ったドキュメント１１にＡＣＬ１２を付与してドキュメント管理ＤＢ２３に格納する。

【０１４６】

この第３の実施形態にかかる電子ファイル管理装置５０６が、管理しているドキュメントに対してユーザからアクセス要求を受けた時の動作について、図８（Ｂ）を参照して説明する。

【０１４７】

ドキュメント管理プログラム６１は、ドキュメントに対するアクセス要求を受けるとユーザ認証を行い、ドキュメント１１に付与されているＡＣＬ１２に基づいてそのユーザにアクセス権限があるかどうか確認する。そのユーザにアクセス権限がある場合、ドキュメント管理プログラム６１は、ドキュメント管理ＤＢ２３から指定されたドキュメント１１とＡＣＬ１２を取り出し、ドキュメント保護プログラム５１１に渡して保護ドキュメント１３を上述のように生成させて受け取り、その生成された保護ドキュメント１３をドキュメント管理プログラム６１への呼び出し側へ返す。すなわち、電子ファイル管理装置５０６から上述のように表示装置などに出力する。

【０１４８】

なお、この第３の実施形態においても、上述した第１の実施形態と同様に、ＡＣＬ１２のＡｃｃｅｓｓ　ｔｙｐｅとして例えばＧｅｔＯｒｉｇｉｎａｌ（オリジナル電子ファイルへのアクセス権限）を定義し、電子ファイル管理装置５０６がユーザ認証を行うことで、ＧｅｔＯｒｉｇｉｎａｌのアクセス権限が認められているユーザに対して、保護ドキュメント１３ではなく、ドキュメント１１を返す（要求に応じて出力する）ようにしてもよい。

【０１４９】

図１３（Ａ）及び図１３（Ｂ）に示す電子ファイル管理装置５０６の他の例を図１４で説明する。図１４は、本発明の第３の実施形態に係る電子ファイル管理装置の他の例を示す図である。図１４（Ａ）及び図１４（Ｂ）に示す電子ファイル管理装置５０６－２において、オリジナルのドキュメント１１－２のみを管理するようにすることもできる。

【０１５０】

図１４（Ａ）において、ドキュメント管理プログラム６１がドキュメント１１－２のみを受け取って保存する際、ドキュメント管理プログラム６１は、受け取ったドキュメント

１１－２を、直接ドキュメント管理ＤＢ２３に格納する。また、図１４（Ｂ）において、ドキュメント管理プログラム６１は、ユーザからのドキュメント・ペアに対してではなく、ドキュメント１１－２に対するアクセス要求に対してドキュメント１１－２を表示装置などに出力する。この場合、ユーザの認証を行っても良いが、ＡＣＬ１２との比較によるユーザのｒｅａｄ権限の判断は行わない。

【０１５１】

次に、第３の実施形態に係るドキュメント管理プログラム６１によって実現される機能構成について図１５で説明する。図１５は、第３の実施形態に係るドキュメント管理プログラムによって実現される機能構成を示す図である。図中、クライアントｃ１及びｃ２は、同一クライアントであってもよい。

【０１５２】

図１５において、ドキュメント管理プログラム６１は、予め保護ドキュメントを１３生成しておくのではなく、ユーザからのアクセス要求があったときに動的に保護ドキュメント１３を生成する。ドキュメント管理プログラム６１によって、少なくとも、ドキュメント保管要求受付部６１ａと、ドキュメント保管部６１ｂと、保護ドキュメント取得部６１ｃと、ドキュメント参照要求受付部６１ｄと、ドキュメント取得部６１ｅとが機能として構成される。

【０１５３】

ドキュメント保管要求受付部６１ａは、ドキュメント保管要求を行ったクライアントｃ１からドキュメント保管要求と共に、ドキュメント１３、ＡＣＬ１２を受け取ると、そのドキュメント１１とＡＣＬ１３をドキュメント保管部６１ｂに渡す。

【０１５４】

ドキュメント保管部６１ｂは、受け取ったドキュメント１１をドキュメント管理ＤＢ２３に格納し、受け取ったＡＣＬ１２を格納したドキュメント１１に設定して、そのドキュメント１１を識別するドキュメントＩＤを返す。

【０１５５】

そして、ドキュメント保管要求受付部６１ａは、ドキュメントＩＤをドキュメント保管要求を行ったクライアントｃ１に返す。

【０１５６】

ドキュメント参照要求受付部６１ｄは、ドキュメント参照要求を行ったクライアントｃ１からドキュメント参照要求とともにドキュメントＩＤを受け取ると、ドキュメント取得部６１ｅにドキュメントＩＤを渡す。

【０１５７】

ドキュメント取得部６１ｅは、受け取ったドキュメントＩＤに該当するドキュメント１１に付与されているＡＣＬ１２を参照し、アクセスを要求しているユーザに参照する権限があるかどうか確認する。権限がある場合には、ドキュメントＩＤに該当するドキュメント１１をドキュメント管理ＤＢ２３から取得する。取得したドキュメント１１とＡＣＬ１２を保護ドキュメント取得部６１ｃに渡す。

【０１５８】

保護ドキュメント取得部６１ｃは受け取ったドキュメント１１とＡＣＬ１２をドキュメント保護プログラム５１１に渡して保護ドキュメント１３を取得して保護ドキュメント取得部６１ｃに返す。

【０１５９】

保護ドキュメント取得部６１ｃは、受け取った保護ドキュメント１３をドキュメント取得部６１ｃに渡す。ドキュメント取得部６１ｅは、受け取った保護ドキュメント１３をドキュメント参照要求受付部６１ｄに渡す。

【０１６０】

ドキュメント参照要求受付部６１ｄは、受け取った保護ドキュメント１３をドキュメント参照要求を行ったクライアントｃ２に返す。

【０１６１】

参照する権限がないユーザは、結局、保護ドキュメント１３にアクセスできないのだから権限を確認せずに誰にでも保護ドキュメント１３を取得して渡すようにしても良い。ただし、暗号化されているとはいえ、保護ドキュメント１３を渡してしまうことは暗号を力ずくで解読するチャンスを与えることになるため、上記のようにアクセス権のないユーザには保護ドキュメントすらアクセスさせないようにするのは意味がある。

【０１６２】

本実施形態によれば、ドキュメント管理プログラム６１により管理・格納されているドキュメントに対するアクセス制御（アクセス権限の制限）と、ユーザに渡された（装置本体６ａから出力された）ドキュメント（ポータブルドキュメント）へのアクセス制御とを統一することができる。

【０１６３】

また、使用するディスク領域を保護ドキュメント１３の分だけ小さくすることができるため、ディスク容量が比較的小さい場合であっても好適な管理ができるようになる。

【０１６４】

次に、本発明の第４の実施形態としての電子ファイル管理装置５０７について、図１６を参照して説明する。図１６は、本発明の第４の実施形態に係る電子ファイル管理装置を示す図である。

【０１６５】

この第４の実施形態における電子ファイル管理装置５０７では、ドキュメント管理プログラム７１が、第１の実施形態でドキュメント保護プログラム５１１に保護ドキュメント１３を生成させて、ドキュメント管理ＤＢ２３にドキュメント１１と保護ドキュメント１３（ドキュメント・ペア）をＡＣＬ１２に関連付けて格納していたのに対し、予めドキュメント保護プログラム５１１に保護ドキュメント１３を生成させて保存し、ドキュメント管理ＤＢ２３にドキュメント１１と保護ドキュメント１３（ドキュメント・ペア）とをＡＣＬ１２に関連付けて格納する。

【０１６６】

すなわち、電子ファイル管理装置５０７が内部でドキュメント保護プログラム５１１を実行するのは、処理のパフォーマンス面から難しくなることも考えられる。そのような場合であっても、あらかじめドキュメント保護プログラム５１１によってプロテクトした保護ドキュメント１３をドキュメント管理プログラム７１により保存することで、ドキュメント１１と保護ドキュメント１３を適切に管理することができるようにするものである。

【０１６７】

この第４の実施形態の電子ファイル管理装置５０７は、物理的な構成は上述した第１の実施形態と同様であり、図１６に示すように、ドキュメント管理プログラム７１と、ドキュメント保護プログラム５１１と、ドキュメント管理ＤＢ２３と、をＨＤＤなどの記憶部（不図示）に備えてなる。

【０１６８】

上述した第１の実施形態と同様のものについては同じ符号とし、説明を省略する。

【０１６９】

また、ドキュメント保護プログラム２２がドキュメント１１から保護ドキュメント１３を生成する動作や、ユーザからのアクセスにより出力された保護ドキュメント１３を復号してプリンタにより印刷する際のシステムや動作も、図３、図５から図８を用いて上述したものと同様であってよい。

【０１７０】

この第４の実施形態にかかる電子ファイル管理装置５０７における電子ファイル格納時の動作について、図１６（Ａ）を参照して説明する。

【０１７１】

ユーザはまず、ドキュメント保護プログラム５１１にドキュメント１１とＡＣＬ１２とを渡して保護ドキュメント１３を生成させる。

【０１７２】

ドキュメント管理プログラム７１にドキュメント１１とＡＣＬ１２と生成された保護ドキュメント１３とを渡し、ユーザが入力装置から格納するよう操作すると、ドキュメント管理プログラム７１は、受け取ったドキュメント１１と保護ドキュメント１３（ドキュメント・ペア）をドキュメント管理ＤＢ２３に格納し、受け取ったＡＣＬ１２を付与して管理する。

【０１７３】

この第４の実施形態にかかる電子ファイル管理装置５０７が、管理しているドキュメントに対してユーザからアクセス要求を受けた時の動作について、図１６（Ｂ）を参照して説明する。

【０１７４】

ドキュメント管理プログラム７１は、ドキュメント・ペアに対するアクセス要求を受けるとユーザ認証を行い、ドキュメント・ペアに付与されているＡＣＬ１２に基づいてアクセス権限があるかどうかを確認する。アクセス権限がある場合には、ドキュメント管理ＤＢ２３に格納している保護ドキュメント１３を返す。すなわち、電子ファイル管理装置５０７から上述のように表示装置などに出力する。

【０１７５】

なお、この第４の実施形態においても、上述した第１の実施形態と同様に、ＡＣＬ１２のＡｃｃｅｓｓ　ｔｙｐｅとして例えばＧｅｔＯｒｉｇｉｎａｌ（オリジナル電子ファイルへのアクセス権限）を定義し、電子ファイル管理装置７がユーザ認証を行うことで、ＧｅｔＯｒｉｇｉｎａｌのアクセス権限が認められているユーザに対して、保護ドキュメント１３ではなく、ドキュメント１１を返す（要求に応じて出力する）ようにしてもよい。

【０１７６】

また、この第４の実施形態では、ドキュメント保護プログラム５１１は電子ファイル管理装置５０７に替えて、他の装置に実装されていてもよい。この場合、ドキュメント保護プログラム５１１が実装された装置でドキュメント１１から保護ドキュメント１３を生成し、その生成を行った装置からネットワークや情報記録媒体などにより電子ファイル管理装置５０７にドキュメント１１と、保護ドキュメント１３と、ＡＣＬ１２とを渡すこととなる。

【０１７７】

また、ドキュメント管理プログラム７１への保存の際にドキュメント１１と保護ドキュメント１３を両方渡すのではなく、保護ドキュメント１３のみを渡してドキュメント１１を破棄するようにしてもよい。この場合、ユーザからのアクセス要求を受けた際には、上述した第２の実施形態と同様の動作となる。

【０１７８】

本実施形態によれば、ドキュメント管理プログラム７１により管理・格納されているドキュメントに対するアクセス制御（アクセス権限の制限）と、ユーザに渡された（電子ファイル管理装置５０７から出力された）ドキュメント（ポータブルドキュメント）へのアクセス制御とを統一することができる。

【０１７９】

また、ドキュメント保護プログラム５１１による保護ドキュメント１３の生成を、電子ファイル管理装置５０７における他の重い処理と同時にならないよう行うことができるため、電子ファイル管理装置５０７の処理能力が比較的低い場合であっても保護ドキュメント１３の生成などの処理を適切に行うことができる。

【０１８０】

また、ドキュメント保護プログラム５１１による保護ドキュメント１３の生成を他の装置で行うことにより、生成などの処理にかかる負担を効果的に分散させることができる。このことにより、電子ファイル管理装置５０７や上記他の装置の処理能力が比較的低い場合であっても、保護ドキュメント１３の生成などの処理を適切に行うことができる。

【０１８１】

図１６（Ａ）及び図１６（Ｂ）に示す電子ファイル管理装置５０７の他の例を図１７で

説明する。図１７は、本発明の第４の実施形態に係る電子ファイル管理装置の他の例を示す図である。図１７（Ａ）及び図１７（Ｂ）に示す電子ファイル管理装置５０７－２において、オリジナルのドキュメント１１－２のみを管理するようにすることもできる。

【０１８２】

図１７（Ａ）において、ドキュメント管理プログラム７１がドキュメント１１－２のみを受け取って保存する際、ドキュメント管理プログラム７１は、受け取ったドキュメント１１－２を、直接ドキュメント管理ＤＢ２３に格納する。また、図１４（Ｂ）において、ドキュメント管理プログラム７１は、ユーザからのドキュメント・ペアに対してではなく、ドキュメント１１－２に対するアクセス要求に対してドキュメント１１－２を表示装置などに出力する。この場合、ユーザの認証を行っても良いが、ＡＣＬ１２との比較によるユーザのｒｅａｄ権限の判断は行わない。

【０１８３】

次に、第４の実施形態に係るドキュメント管理プログラム７１によって実現される機能構成について図１８で説明する。図１８は、第４の実施形態に係るドキュメント管理プログラムによって実現される機能構成を示す図である。図中、クライアントｃ１－２及びｃ２は、同一クライアントであってもよい。

【０１８４】

図１８において、ドキュメント管理プログラム７１によって、少なくとも、ドキュメント保管要求受付部７１ａと、ドキュメント保管部７１ｂと、ドキュメント参照要求受付部７１ｄと、ドキュメント取得部７１ｅとが機能として構成される。

【０１８５】

また、ドキュメント管理プログラム７１の外部で保護ドキュメント１３を作成してから保管する仕組みの場合、ドキュメント保管要求を行うクライアントｃ１－２は、ドキュメント保管要求部７１ｆと、保護ドキュメント取得部７１ｇとを有する。

【０１８６】

ドキュメント保管要求部７１ｆは、保護ドキュメント取得部７１ｇにドキュメント１１とＡＣＬ１２とを渡す。保護ドキュメント取得部７１ｇは受け取ったドキュメント１１とＡＣＬ１２をドキュメント保護プログラム５１１に渡して保護ドキュメント１３を取得し、その保護ドキュメント１３をドキュメント保管要求部７１ｆに返す。

【０１８７】

ドキュメント保管要求部７１ｆは、ドキュメント保管要求を行うクライアントｃ１－２として、ドキュメント管理プログラム７１にドキュメント保管要求とともにドキュメント１１と、保護ドキュメント１３と、ＡＣＬ１２とを渡す。

【０１８８】

ドキュメント管理プログラム７１のドキュメント保管要求受付部７１ａは、ドキュメント保管要求を行ったクライアントｃ１－２からドキュメント保管要求とともにドキュメント１１と、保護ドキュメント１３と、ＡＣＬ１２とを受け取ると、それらをドキュメント保管部７１ｂに渡す。

【０１８９】

ドキュメント保管部７１ｂは、受け取ったドキュメント１１と保護ドキュメントとをドキュメント・ペアとしてドキュメント管理ＤＢ２３に格納し、そのドキュメント・ペアに受け取ったＡＣＬ１２を付与する。ドキュメント・ペアの識別子をドキュメントＩＤとしてドキュメント保管要求受付部７１ａに返す。

【０１９０】

ドキュメント保管要求受付部７１ａは、ドキュメントＩＤをドキュメント保管要求をしたクライアントｃ１－２に返す。

【０１９１】

ドキュメント管理プログラム７１において、ドキュメント参照要求を行うクライアントｃ２からドキュメント参照要求を受け取ったときの流れは図４と同様であるので、説明を省略する。

【０１９２】
次に、上述した各実施形態で、印刷用端末５０３に接続されたプリンタ５０２から機密印刷にて出力させる場合について説明する。
【０１９３】
先ず、上記各実施形態において適用されるプリンタが備えるセキュリティ機能の一部を図１９で説明する。図１９は、プリンタが備えるセキュリティ機能の例を示す図である。
【０１９４】
図１９において、まず、印刷要件としてＰＡＣが設定されている場合のドキュメント印刷プログラム５２１の動作について説明する。ＰＡＣが設定されている場合のドキュメント印刷プログラム５２１の動作を図２０に示す。
【０１９５】
（１）ドキュメント印刷プログラム５２１はＰＡＣが設定されているドキュメントファイルを印刷する際には、図２１に示すように、プリントダイアログ５５８を表示させた後に個人識別番号（Personal Identification Number：ＰＩＮ）を入力するＰＩＮ入力ダイアログ５５９を印刷用端末５０３の表示装置に表示させ、ユーザにＰＩＮの入力を要求する。
【０１９６】
（２）印刷用端末５０２の入力装置を用いてユーザがＰＩＮを入力すると、ドキュメント印刷プログラム５２１は、これをプリンタドライバ５０３ｂに設定し、印刷を指示する。
【０１９７】
プリンタドライバ５０３ｂは、ドキュメントからPostscriptＰＤＬ（Page Description Language）で記述された印刷データ（ＰＤＬデータ）を生成し、印刷部数や出力トレイなどの印刷ジョブ情報を記述したＰＪＬ（Print Job Language）データをＰＤＬデータの先頭に付加する。プリンタドライバ５０３ｂはさらにＰＪＬデータの一部としてＰＩＮを付加し、そのＰＪＬデータ付きＰＤＬデータをプリントエンジン５０３ａに送る。
【０１９８】
プリンタ５０３は、ＰＪＬデータ付きＰＤＬデータを受け取るとＰＪＬデータの内容を参照し、機密印刷用のＰＩＮが含まれている場合は印刷出力せずにプリンタ５０３内部の記憶装置（ＨＤＤなど）にＰＪＬデータ付きＰＤＬデータを保存する。ユーザがＰＩＮをプリンタ５０３のオペレーションパネルを介して入力すると、プリンタ５０３は入力されたＰＩＮをＰＪＬデータに含まれるＰＩＮと照合し、一致すればＰＪＬデータに含まれていた印刷ジョブ条件（部数、トレイなど）を適用しながらＰＤＬデータに従って印刷出力する。
【０１９９】
（３）プリンタドライバ５０３ｂにＰＩＮが設定できない、すなわち、プリンタ３３が機密印刷をサポートしていない場合には、機密印刷をサポートしている別のプリンタを選択するようにユーザに通知し、ドキュメントを印刷せずに処理を終了する。
【０２００】
このようにすることで、印刷実行後、プリンタ５０３のオペレーションパネルにおいて印刷実行前に入力したものと同一のＰＩＮが入力されるまでドキュメントのプリントアウトがプリンタ５０３から出力されなくなる。このため、ドキュメントのプリントアウトがプリンタ５０３に不用意に放置されることがなくなり、プリントアウトによるドキュメントの漏洩を防止することが可能となる。
【０２０１】
さらに、ネットワーク上を流れるプリントデータを盗聴されないようにプリンタ５０３とやりとりをＳＳＬで保護してもよい。
【０２０２】
また、ドキュメント印刷プログラム５２１をWindows（登録商標）Domainのユーザ管理

と連動させて、ユーザに対してＰＩＮの入力を要求しないようにしてもよい。例えば、ＰＩＮをユーザに入力させるのではなく、Windows（登録商標）Domainから現在ログオン中のユーザＩＤを取得し、プリントデータとともにユーザＩＤをプリンタ５０３へ送付するようにする。プリンタ５０３は、オペレーションパネルでユーザからのパスワード入力を受け、そのユーザＩＤとパスワードとでWindows（登録商標）Domainのユーザ認証機構を用いてユーザ認証を行い、成功すればプリントアウトするようにしても良い。Windows（登録商標）Domainに限定されず、予め導入されているユーザ管理と連動させることで、ユーザにとって面倒なＰＩＮ入力の手間を削減できる。

【０２０３】

次に、印刷要件としてＥＢＣが設定されている場合のドキュメント印刷プログラム５２１の動作について説明する。

【０２０４】

（１）ドキュメント印刷プログラム５２１は、ＥＢＣが設定されているドキュメントを印刷する際にドキュメントＩＤを示すバーコード画像データ（又は、二次元コード）のデータを生成する。

【０２０５】

（２）ドキュメント印刷プログラム５２１は、生成したバーコード画像データをスタンプ画像としてプリンタドライバ５０３ｂにセットし、プリンタ５０３に印刷を指示する。

【０２０６】

（３）プリンタドライバ５０３ｂにＥＢＣが設定できない、すなわち、プリンタ５０３がスタンプ機能をサポートしていない場合は、スタンプ機能をサポートしている他のプリンタを選択するようにユーザに通知し、印刷を行わずに処理を終了する。

【０２０７】

このようにすることで、ドキュメントのプリントアウトの各ページにはバーコードが印刷されるため、このバーコードを識別できる複写機、ファックス、スキャナのみがバーコードをデコードすることでドキュメントＩＤを取得し、そのドキュメントＩＤを基にアクセスコントロールサーバ５０４が、ハードコピー、画像読み取り、ファックス送信などが許可されているか否かを判断することが可能となる。これにより、紙文書まで一貫したセキュリティ確保が可能となる。

【０２０８】

次に、印刷要件としてＢＤＰが設定されている場合のドキュメント印刷プログラム５２１の動作について説明する。

【０２０９】

（１）ドキュメント印刷プログラム５２１は、ＢＤＰが設定されているドキュメントを印刷する際に、印刷を要求しているユーザ名と印刷日時とを文字列として取得する（例えば、Ichiro,2002/08/04 23:47:10）。

【０２１０】

（２）ドキュメント印刷プログラム５２１は、ドキュメントのプリントアウトを複写機で複写した際に、生成した文字列が浮き上がるように地紋画像を生成する。

【０２１１】

（３）ドキュメント印刷プログラム５２１は、生成した地紋画像をスタンプとしてプリンタドライバ５０３ｂにセットし、プリンタ５０３にドキュメントの印刷を指示する。

【０２１２】

（４）プリンタドライバ５０３ｂにＢＤＰが設定できない場合、すなわちプリンタ５０３が地紋印刷をサポートしていない場合には、地紋印刷をサポートしている別のプリンタを選択するようにユーザに通知し、印刷を行わずに処理を終了する。

【０２１３】

このようにすることで、ドキュメントのプリントアウトの各ページには、印刷処理を実行したユーザ名と日時とが浮き出る地紋として印刷され、プリントアウトを複写機やスキャナ、ファックスで処理すると文字列が浮き出ることとなる。これ、ＥＢＣをサポートし

ていない複写機をしようとする場合などに有効であり、ドキュメントのプリントアウトを複写することによる情報漏洩に対して抑止力を有する。

【０２１４】

次に、印刷要件としてＳＬＳが設定されている場合のドキュメント印刷プログラム５２１の動作について説明する。

【０２１５】

（１）ドキュメント印刷プログラム５２１は、ＳＬＳが設定されているドキュメントファイルを印刷する際に、予め用意された画像のうち、そのドキュメントの機密レベルに応じたもの（Top Secretならば「極秘」のマークなど）を選択する。

【０２１６】

（２）選択した画像のデータを、スタンプとしてプリンタドライバ５０３ｂにセットし、プリンタ５０３に印刷を指示する。

【０２１７】

（３）プリンタドライバ５０３ｂにＳＬＳをセットできない場合、すなわち、プリンタ５０３がＳＬＳをサポートしていない場合には、ラベルスタンプをサポートしている別のプリンタを選択するようにユーザに通知し、印刷を行わずに処理を終了する。

【０２１８】

このようにすることで、ドキュメントファイルのプリントアウトには、自動的に「極秘」や「マル秘」がスタンプとして印刷されるため、ドキュメントが機密文書であることが明らかとなる。すなわち、プリントアウトを所持する者に管理上の注意を喚起することができる。

【０２１９】

上記の各例は、あくまでも印刷要件の一例であり、改ざん防止用の電子透かしを印刷するようにしたり、保護されているドキュメントは特殊な用紙に印刷する（印刷に使用する用紙トレイを特殊用紙のトレイに限定する）ようにしてもよい。

【０２２０】

このように、プリンタ５０３がサポートする様々なセキュリティ機能を利用してセキュリティポリシーを設定することによって、プリンタ５０３のセキュリティ機能を無駄なく活用して、プリントアウトに至るまで一貫したセキュリティの確保が可能となる。これは上述した各実施形態のシステム構成においても同様である。

【０２２１】

上記各実施例において共通のユーザにて提供される画面について図２２から図２６で説明する。

【０２２２】

図２２は、電子ファイル管理装置にアクセスした際に表示される画面例を示す図である。図２２において、例えば、管理者としてのユーザが、ユーザが利用しているクライアントの画面５５０に表示される文書管理５５１を選択すると、ユーザを認証するためのダイアログ５５２が表示される。画面５５２のユーザ名及びパスワードの入力域５５３に、ユーザがユーザ名及びパスワードを入力し、認証を実行するためにＯＫボタン５５４をクリックすると、電子ファイル管理装置５１１にてユーザの認証が行われる。一方、ユーザがキャンセルボタン５５５をクリックすると、電子ファイル管理装置５１１へのアクセスがキャンセルされる。

【０２２３】

ユーザの認証に成功すると、次のように電子ファイル管理装置５０１にて管理されているドキュメントの一覧を、例えば、図２３に示すように表示する。図２３は、電子ファイル管理装置にて管理されるドキュメントの一覧を表示する画面例を示す図である。

【０２２４】

図２３において、画面５６０は、ユーザの認証が成功した場合に表示される場面であって、電子ファイル管理装置５０１にて管理されるドキュメントの一覧を表示する。

【０２２５】

ドキュメントの一覧として、フォルダ１、フォルダ２、フォルダ３、及びフォルダ４、文書０１、文書０２、及び文書０３とが表示される。フォルダ１から４は、例えば、フォルダの形状を示すアイコンで表示され、文書０１から０３は、例えば、サムネイルで表示される。

【０２２６】

例えば、ユーザが文書０２を選択すると、ドキュメント参照要求が電子ファイル管理装置５０１に送信され、文書０２に対するアクセス権が確認される。参照権限がある場合には、文書０２の保護ドキュメントだけをクライアントに提示する。

【０２２７】

図２４は、保護ドキュメントが提示されている画面例を示す図である。図２４において、画面５７０では、文書０２として文書０２の保護ドキュメントが提供されることがアイコン５７１によって示される。例えば、アイコン５７１は、ＰＤＦファイルを示しており、有効の状態で表示されることによって、文書０２の保護ドキュメントしかアクセスできないことを示す。

【０２２８】

文書０２を示すサムネイル５７２では、例えば、左端にオリジナルのドキュメントがＭＳ　Ｗｏｒｄ（登録商標）のファイル形式を示すアイコン５７３が表示される。

【０２２９】

クライアント側では文書０２の保護ドキュメントを開くために、ダイアログ５７４を表示して、再度ユーザ認証が求められる、先のユーザ認証で入力されたものを自動的に使用するようにしても良い。

【０２３０】

ダイアログ５７４に設定された認証情報による認証が生協すると、例えば、図２５に示されるような画面が表示される。図２５は、保護ドキュメントが開かれた状態を示す図である。

【０２３１】

図２５において、画面５８０は、文書０２の保護ドキュメントに対するユーザ認証が成功し、かつ、保護ドキュメントを開く権限があった場合に、開かれた保護ドキュメントを表示する。

【０２３２】

そして、ユーザは、文書０２の保護ドキュメントの内容を参照することができ、更に、印刷権限があればこの保護ドキュメントを印刷することができる。つまり、ユーザが印刷するためのアイコン５８１をクリックすると、印刷権限がこのユーザにあるか否かが確認され、規定されているこの文書０２に対するセキュリティの要件を満たすように処理が行われ印刷される。

【０２３３】

一方、図２４に示す画面５７０において、ユーザがオリジナルの文書０２を参照する場合について図２６で説明する。図２６は、ユーザにオリジナル参照権限が与えられていない場合の画面例を示す図である。

【０２３４】

図２６において、ユーザがアイコン５７５をクリックすることによって、オリジナルの文書０２にアクセスしようとすると、ユーザにオリジナルの文書０２にアクセスする権限があるか否かが判断される。ユーザにオリジナルの文書０２を参照する権限がない場合には、「セキュリティポリシーによるオリジナル参照権限が与えられていません。」等のメッセージを示すダイアログ５７６が表示される。従って、ユーザは、オリジナルの文書０２を参照することができない。

【０２３５】

なお、上述した各実施形態は、本発明の好適な実施形態であり、本発明の主旨を逸脱しない範囲内において、種々変形して実施することが可能である。

【０２３６】

例えば、上述した各実施形態で用いられる各種ドキュメント（電子ファイル）の内容は、文書に限定されず、例えば画像を含めた文書ファイルや画像ファイルなどであってもよい。

【０２３７】

また、本発明に係る電子ファイル管理装置が入力装置と表示装置とを備えることとしているが、この構成に限定されず、例えば、ネットワークを介して接続されたユーザ端末により電子ファイル管理装置がユーザからの入力を受けたり、ネットワークを介して接続された表示装置や外部記録装置に電子ファイル管理装置から出力したりしてもよい。

【０２３８】

また、プリンタを電子ファイル管理装置や印刷用端末に接続して出力に用いる場合、ネットワークを介して接続されたものであっても、電子ファイル管理装置や印刷用端末と一体化されたものであってもよい。

【０２３９】

また、格納装置が複数ある場合、ＡＣＬなどが付与されていることを確認できるのであれば（例えば、上述のように関連付けて格納する、など）、ドキュメント・ペアのそれぞれやＡＣＬを異なる格納部に格納してもよい。

【０２４０】

また、以上に、ドキュメント保護プログラムとしてユーザベース・アクセス制御モデルのものを利用した場合の実施形態について説明したが、アクセス権限を管理するための情報を設定して電子ファイルの管理を行うことができれば本発明はこのものに限定されない。例えば、ポリシーベース・アクセス制御モデルのドキュメント保護プログラムを利用した場合には、ＡＣＬではなくポリシーに従ってアクセスが制御されるだけで基本的には同じ仕組みとして本発明は同様に適用可能である。

【図面の簡単な説明】

【０２４１】

【図１】本発明の第１の実施形態に係る電子ファイル管理装置を示す図である。

【図２】ＡＣＬの構成例を示す図である。

【図３】ドキュメント保護・印刷システムの構成を示す図である。

【図４】第１の実施形態に係るドキュメント管理プログラムによって実現される機能構成を示す図である。

【図５】ドキュメント保護プログラムの動作を示す図である。

【図６】ＡＣＬデータベースに記録される情報の構造例を示す図である。

【図７】ドキュメント印刷プログラム及びアクセスコントロールサーバの動作の流れを示す図である。

【図８】アクセスコントロールへのＳＯＡＰによる問い合わせの例を示す図である。

【図９】本発明の第１の実施形態に係る電子ファイル管理装置の他の例を示す図である。

【図１０】本発明の第２の実施形態に係る電子ファイル管理装置を示す図である。

【図１１】本発明の第２の実施形態に係る電子ファイル管理装置の他の例を示す図である。

【図１２】第２の実施形態に係るドキュメント管理プログラムによって実現される機能構成を示す図である。

【図１３】第３の実施形態の電子ファイル管理装置の例を示す図である。

【図１４】本発明の第３の実施形態に係る電子ファイル管理装置の他の例を示す図である。

【図１５】第３の実施形態に係るドキュメント管理プログラムによって実現される機能構成を示す図である。

【図１６】本発明の第４の実施形態に係る電子ファイル管理装置を示す図である。

【図１７】本発明の第４の実施形態に係る電子ファイル管理装置の他の例を示す図である。

【図１８】第４の実施形態に係るドキュメント管理プログラムによって実現される機能構成を示す図である。
【図１９】プリンタが備えるセキュリティ機能の例を示す図である。
【図２０】ＰＡＣが設定されたドキュメントを印刷する際の処理を示す図である。
【図２１】ＰＩＮ入力のダイアログを示す図である。
【図２２】電子ファイル管理装置にアクセスした際に表示される画面例を示す図である。
【図２３】電子ファイル管理装置にて管理されるドキュメントの一覧を表示する画面例を示す図である。
【図２４】保護ドキュメントが提示されている画面例を示す図である。
【図２５】保護ドキュメントが開かれた状態を示す図である。
【図２６】ユーザにオリジナル参照権限が与えられていない場合の画面例を示す図である。

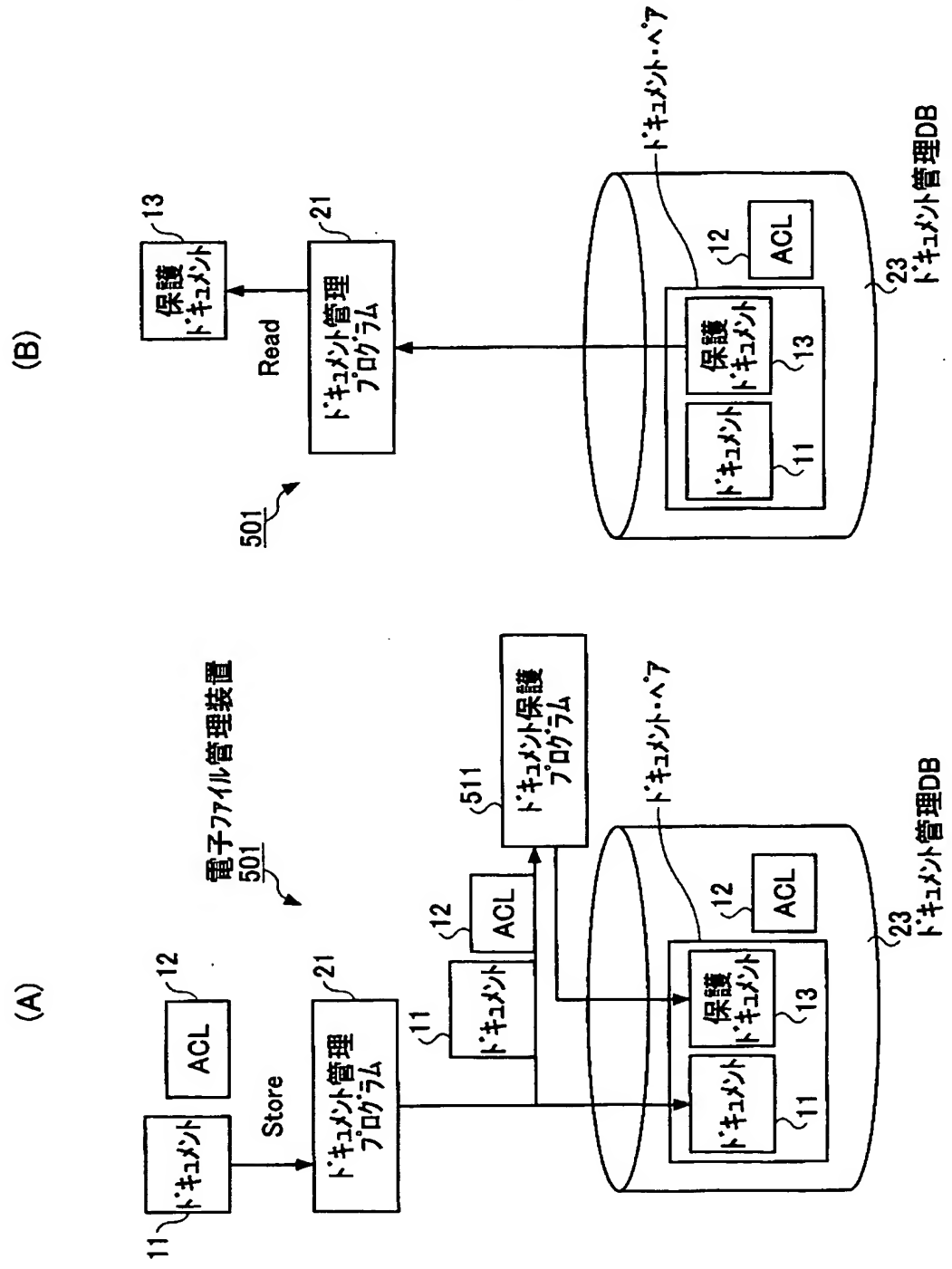
【符号の説明】

【０２４２】

１１	ドキュメント
１２	ＡＣＬ
１３	保護ドキュメント
２１	ドキュメント管理プログラム
２３	ドキュメント管理ＤＢ
５０１	電子ファイル管理装置
５０２	印刷用端末
５０３	プリンタ
５０４	アクセスコントロールサーバ
５１１	ドキュメント保護プログラム
５２１	ドキュメント印刷プログラム
５４１	ユーザデータベース
５４２	ＡＣＬデータベース

【書類名】図面
【図１】

本発明の第1の実施形態に係る電子ファイル管理装置を示す図



【図２】

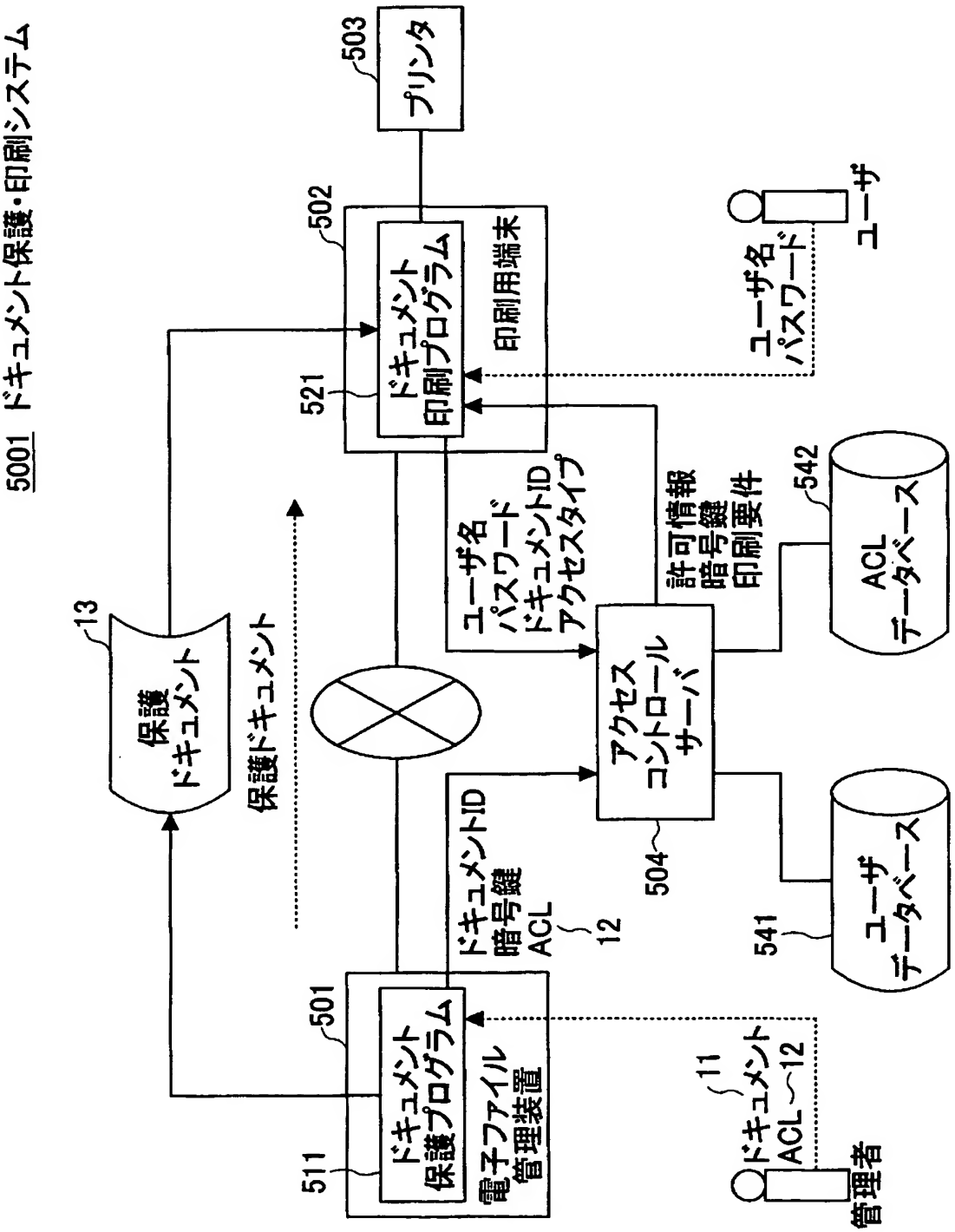
ACLの構成例を示す図

12

User name	Access type	Permission	Requirement
Ichiro	Read	Allowed	－
	Write	Denied	－
	Print	Allowed	PAC(Private Access)
			BDP(Background Dot Patten)
			EBC(Embedding BarCode)
	Hardcopy	Allowed	RAD(Record Audit Date)
Taro	Read	Allowed	－
	Write	Denied	－
	Print	Denied	－
	Hardcopy	Denied	－
⋮			

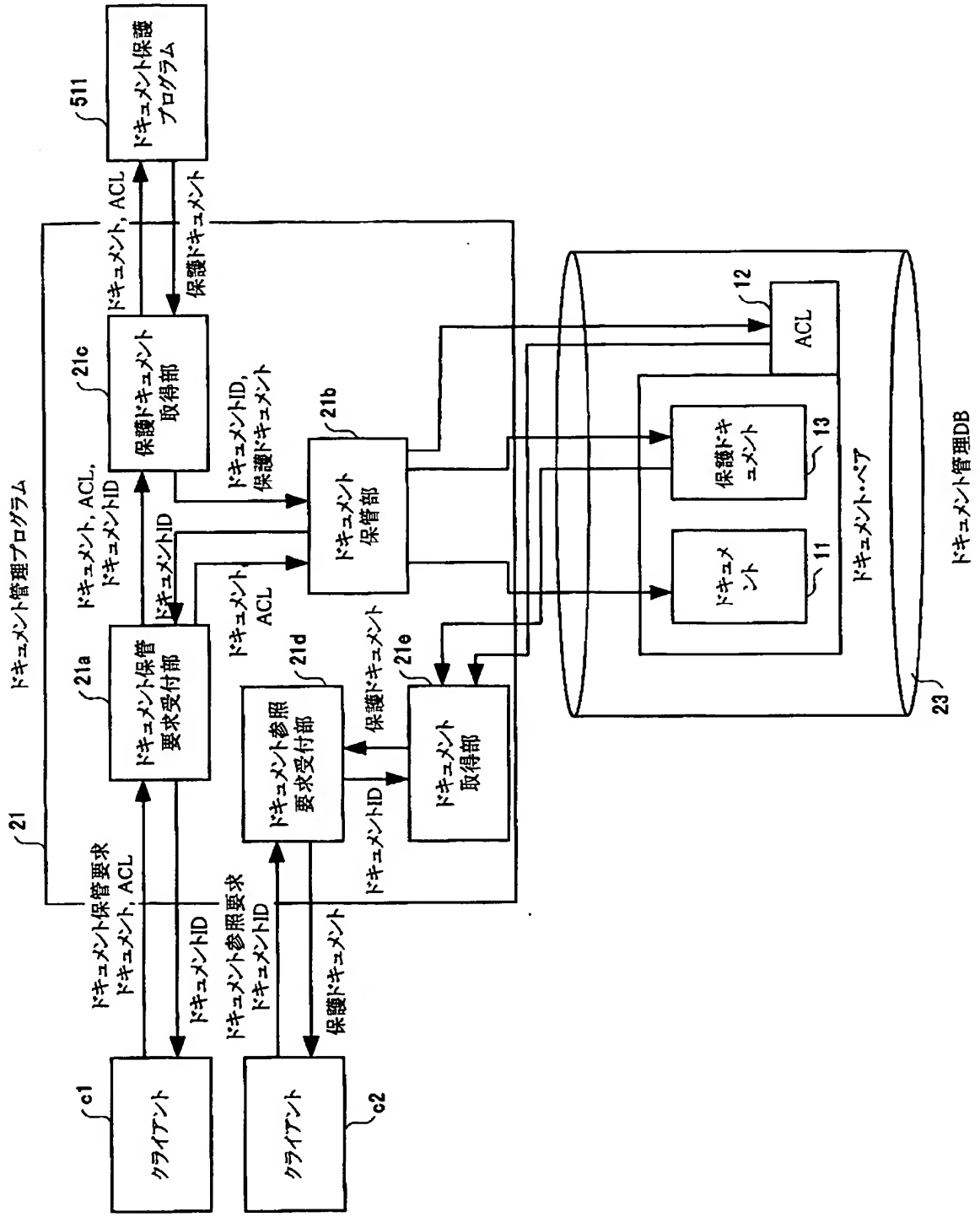
【図３】

ドキュメント保護・印刷システムの構成を示す図



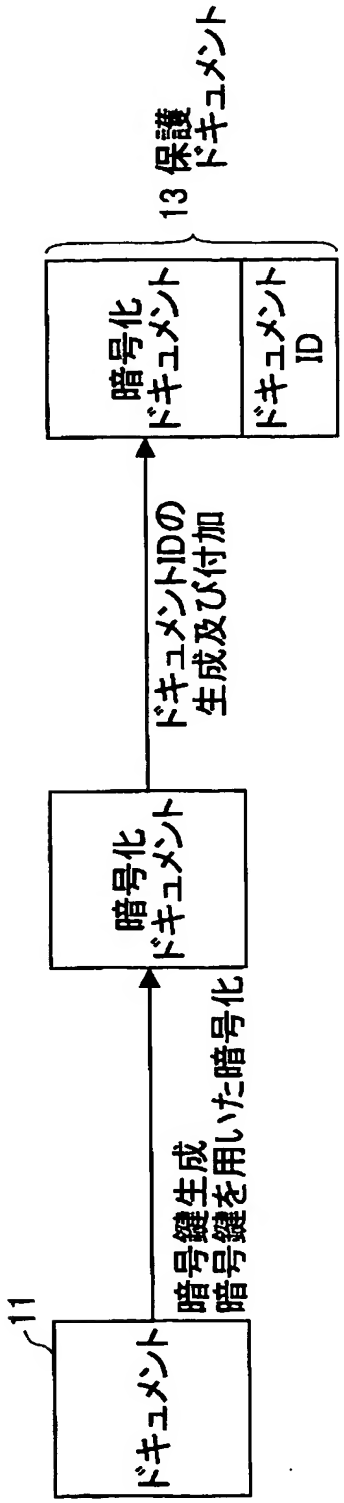
【図４】

第１の実施形態に係るドキュメント管理プログラムによって実現される機能構成を示す図



【図５】

ドキュメント保護プログラムの動作を示す図



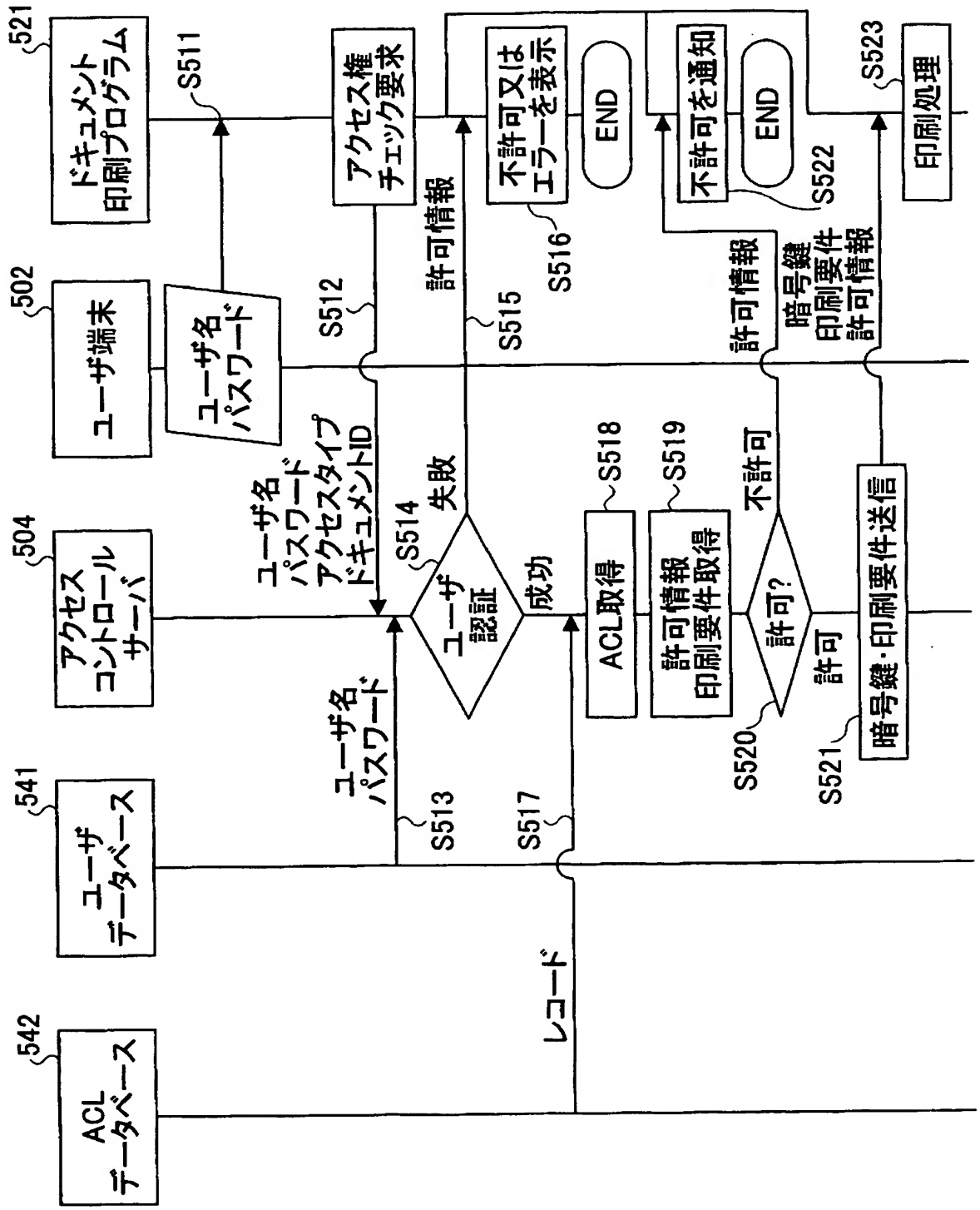
【図６】

ACLデータベースに記録される情報の構造例を示す図

Document ID	Key	ACL
133.139.234.23.22.125.98.192	89FECA8D2B	(binary data)
133.139.234.23.22.125.99.105	A73C44DA59	(binary data)

【図７】

ドキュメント印刷プログラム
及びアクセスコントロールサーバの動作の流れを示す図



【図８】

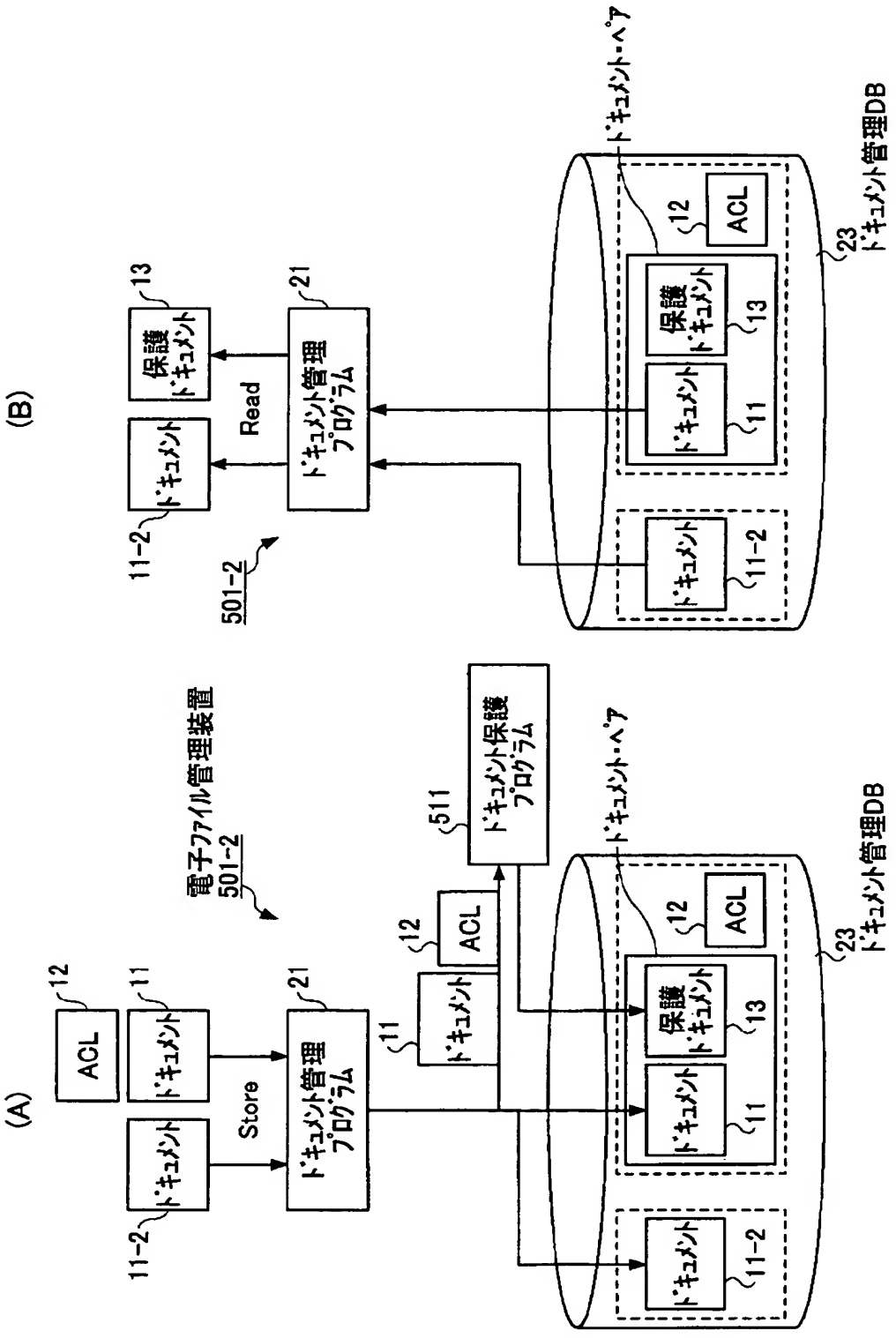
アクセスコントロールへのSOAPによる問い合わせの例を示す図

```
<?xml version="1.0" encoding="UTF-8" ?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
 s:encodingStyle="http://shemas.xmlsoap.org/soap/encoding/">
<s:Body>
<m:isAllowed xmlns:m="http://sample.com/sample">
<sessionId>adfkla;iowoemads</sessionId>
<userId>taro.yamada</userId>
<docId>shm000000000003</docId>
<accessType>print</accessType>
</m:isAllowed>
</s:Body>
</s:Envelope>


<?xml version="1.0" encoding="UTF-8" ?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
s:encodingStyle="http://shemas.xmlsoap.org/soap/encoding/">
<s:Body>
<m:isAllowedResponse xmlns:ns1="http://sample.com/sample">
<isAllowedReturn>
<allowed xsi:type="xsd:boolean">true</allowed>
<requirements>
<item>
<requirement>private_access</requirement>
</item>
<item>
<requirement>watermark</requirement>
<supplement>CONFIDENTIAL</supplement>
</item>
</requirements>
</isAllowedReturn>
</m:isAllowedResponse>
</s:Body>
</s:Envelope>
```

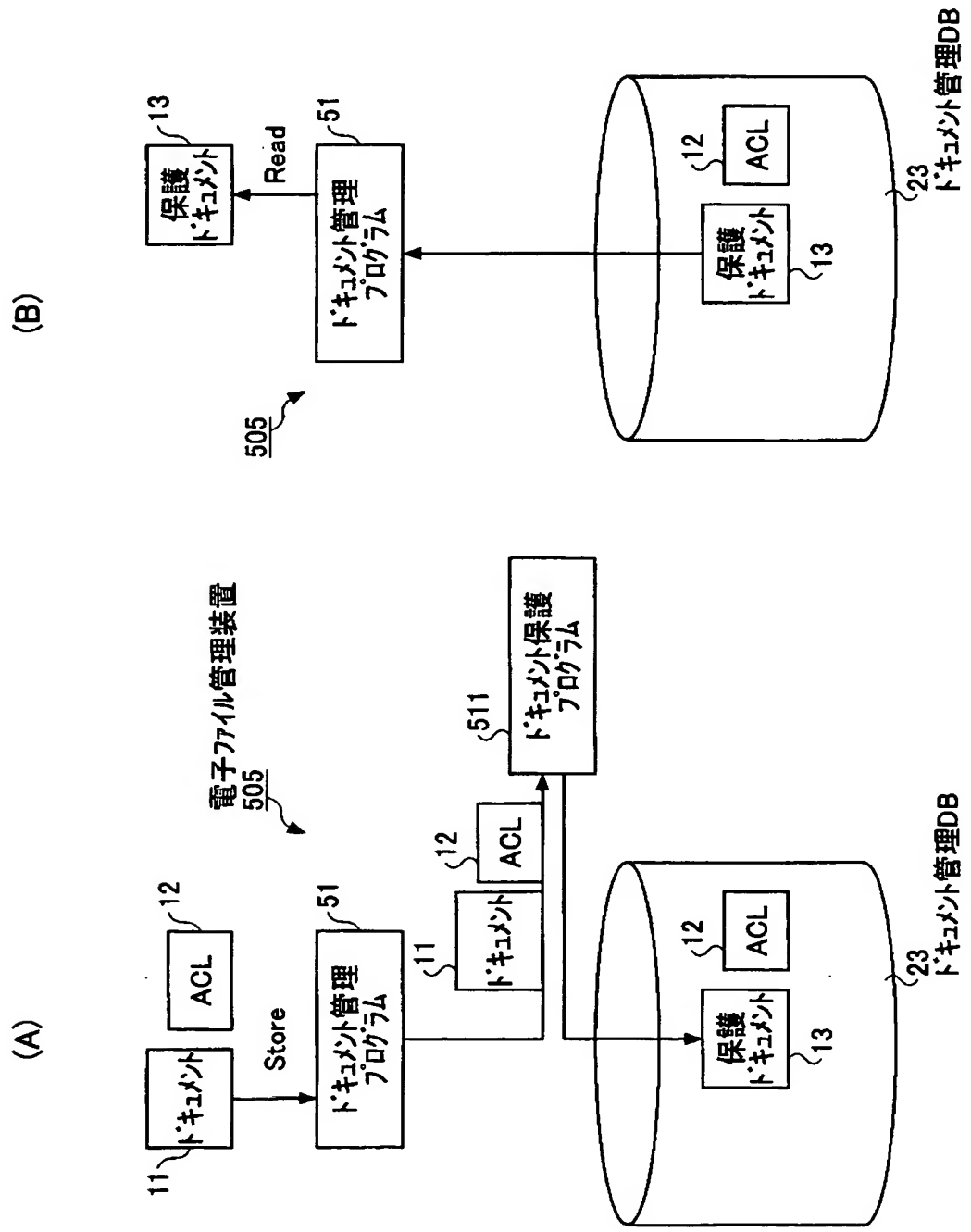
【図９】

本発明の第１の実施形態に係る電子ファイル管理装置の他の例を示す図



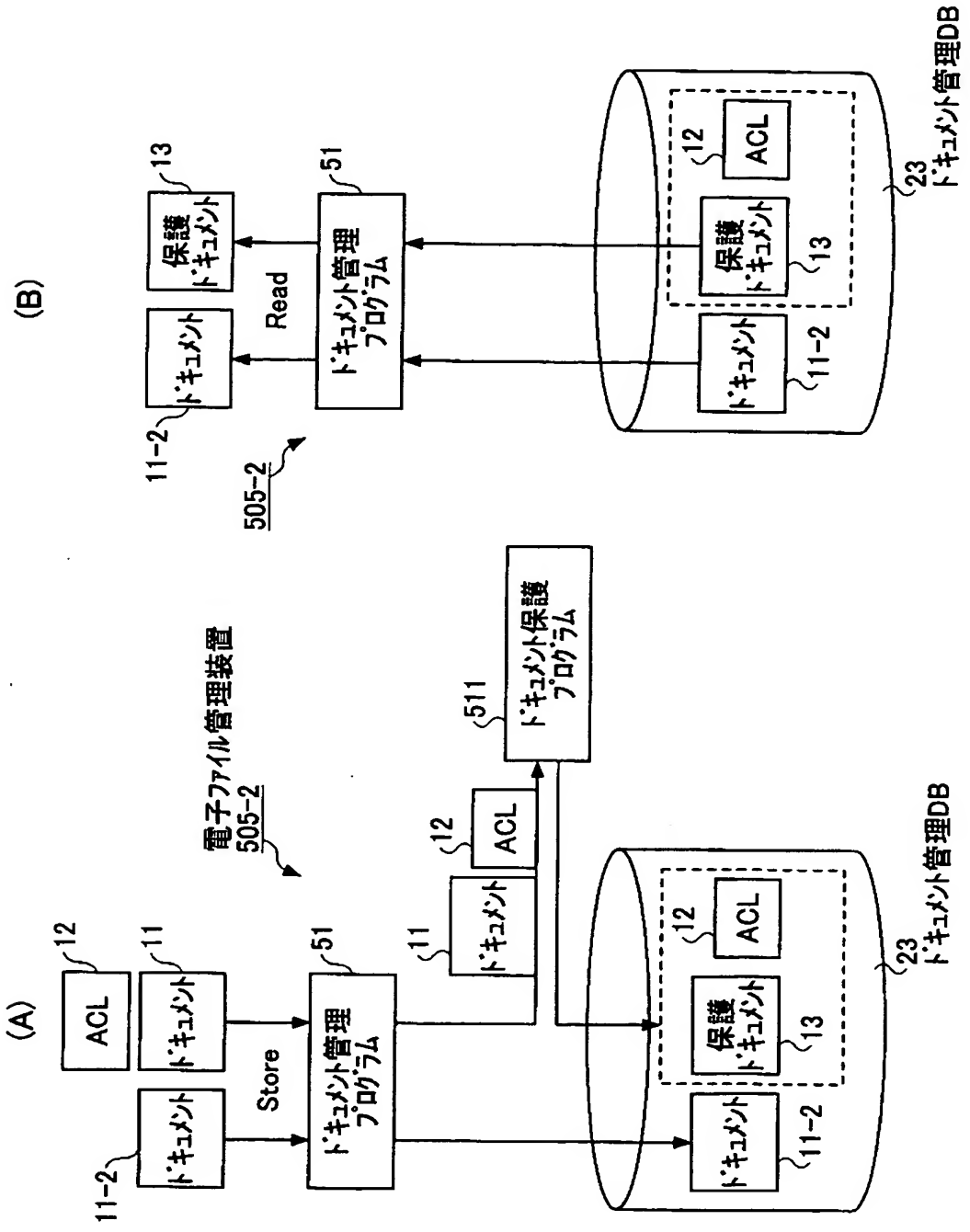
【図１０】

本発明の第2の実施形態に係る電子ファイル管理装置を示す図



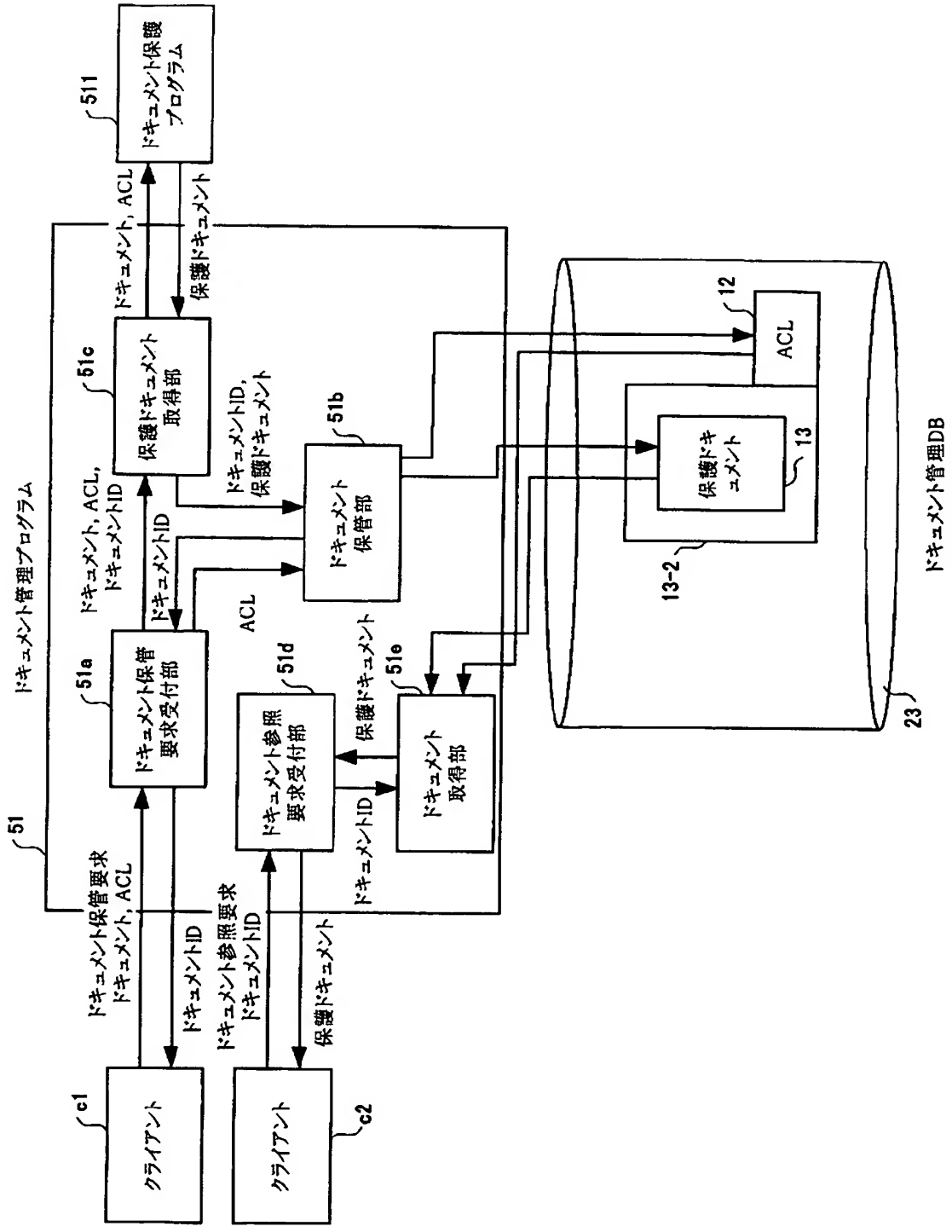
【図１１】

本発明の第2の実施形態に係る電子ファイル管理装置の他の例を示す図



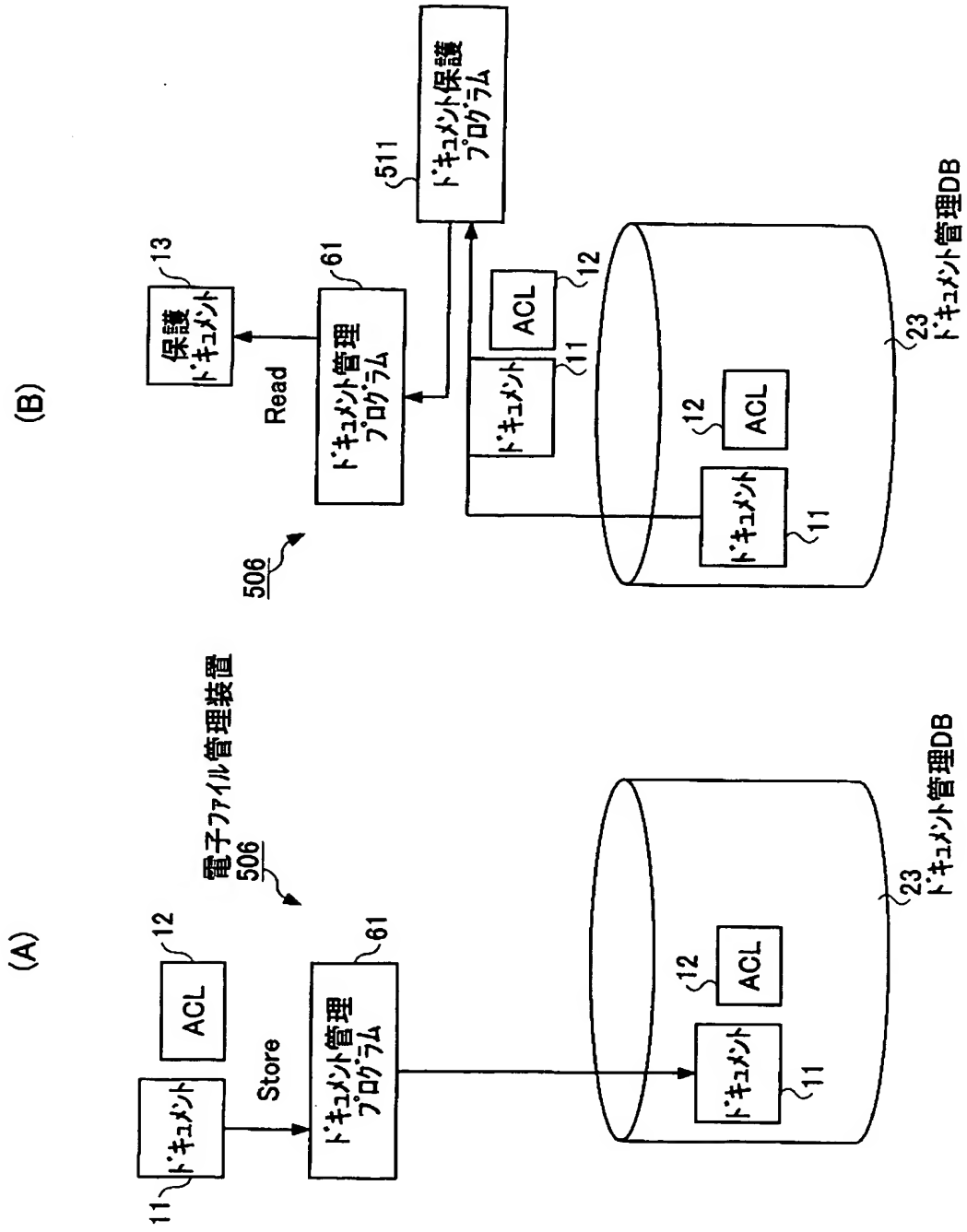
【図１２】

第2の実施形態に係るドキュメント管理プログラムによって実現される機能構成を示す図



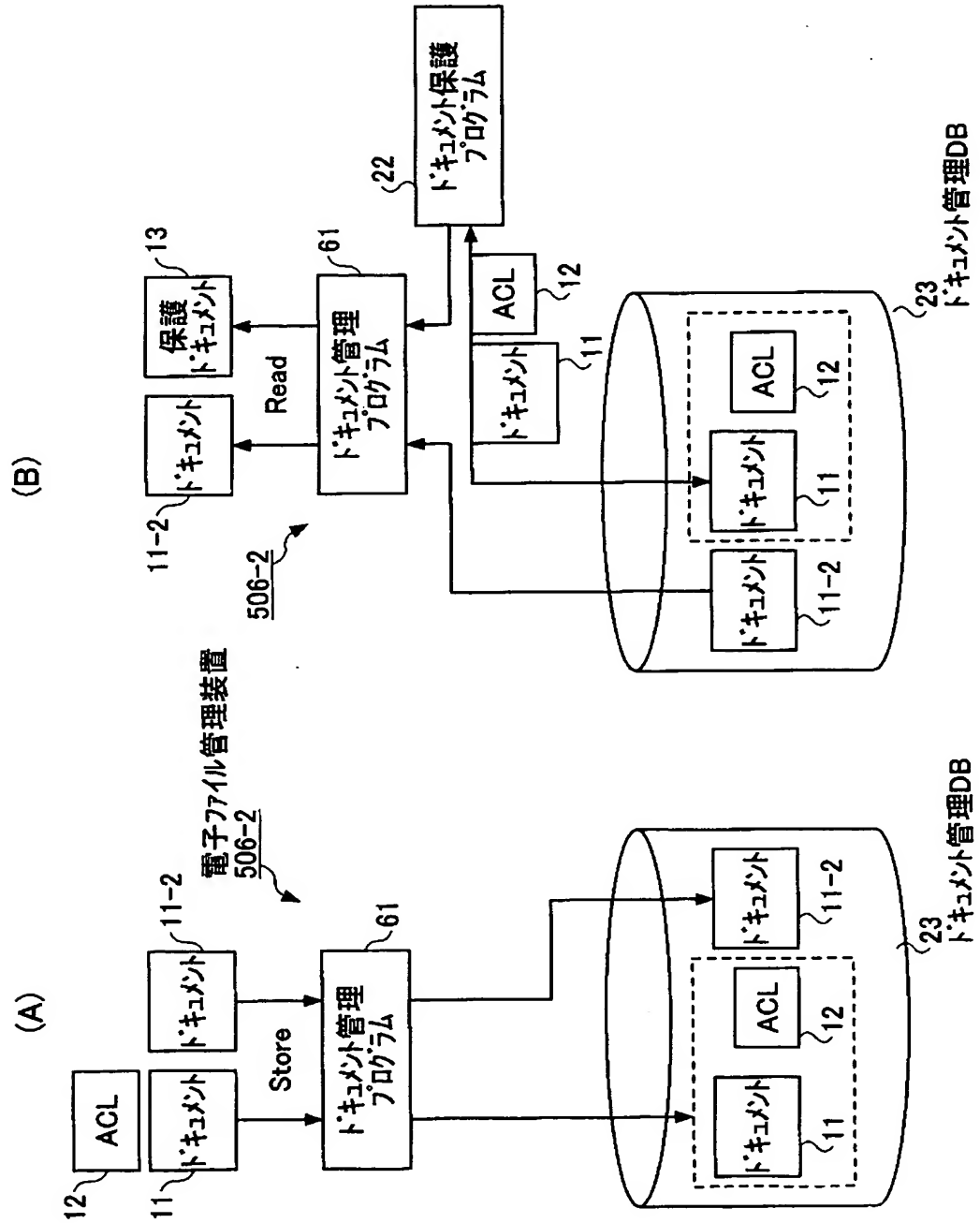
【図１３】

第3の実施形態の電子ファイル管理装置の例を示す図



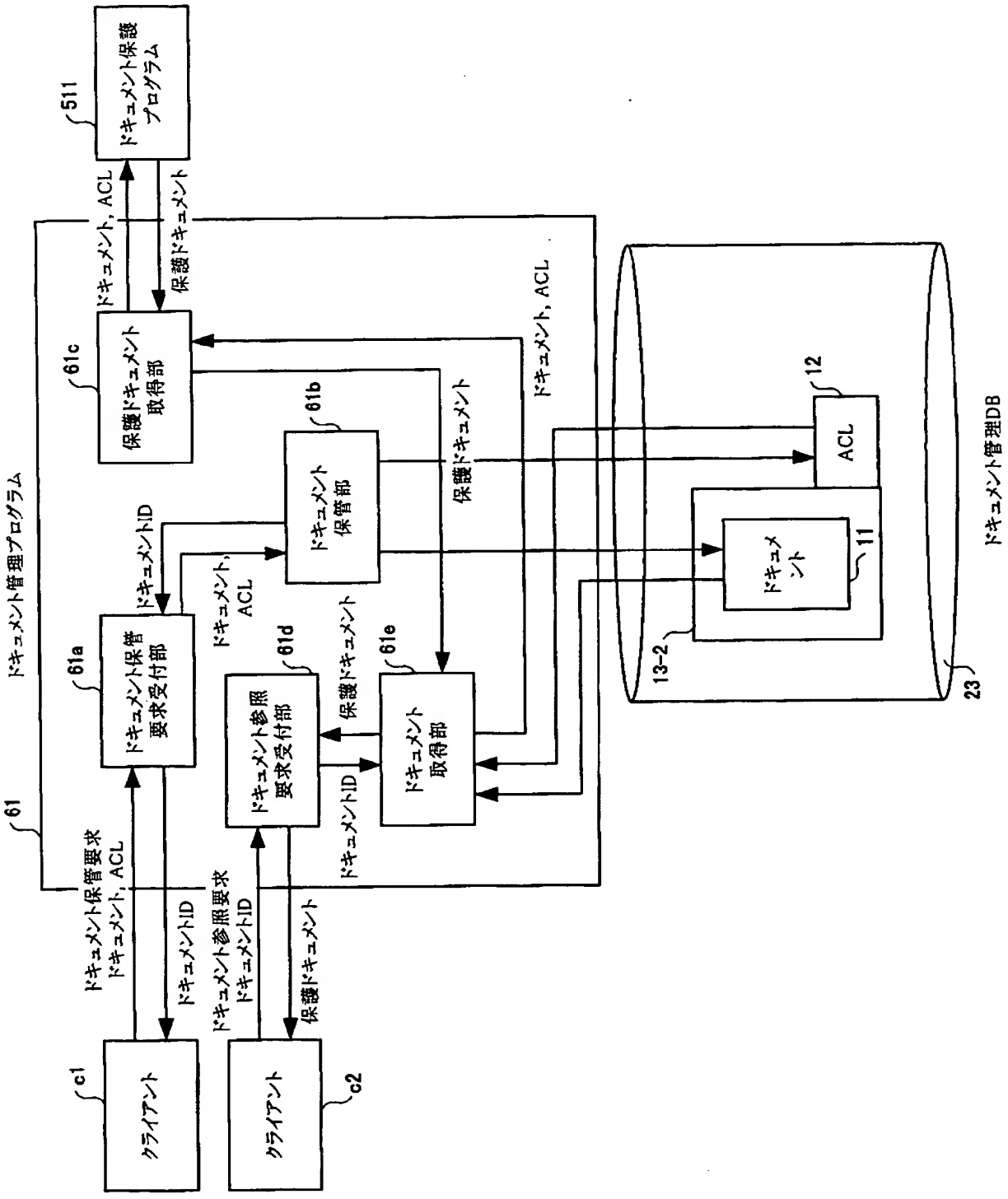
【図１４】

本発明の第3の実施形態に係る電子ファイル管理装置の他の例を示す図



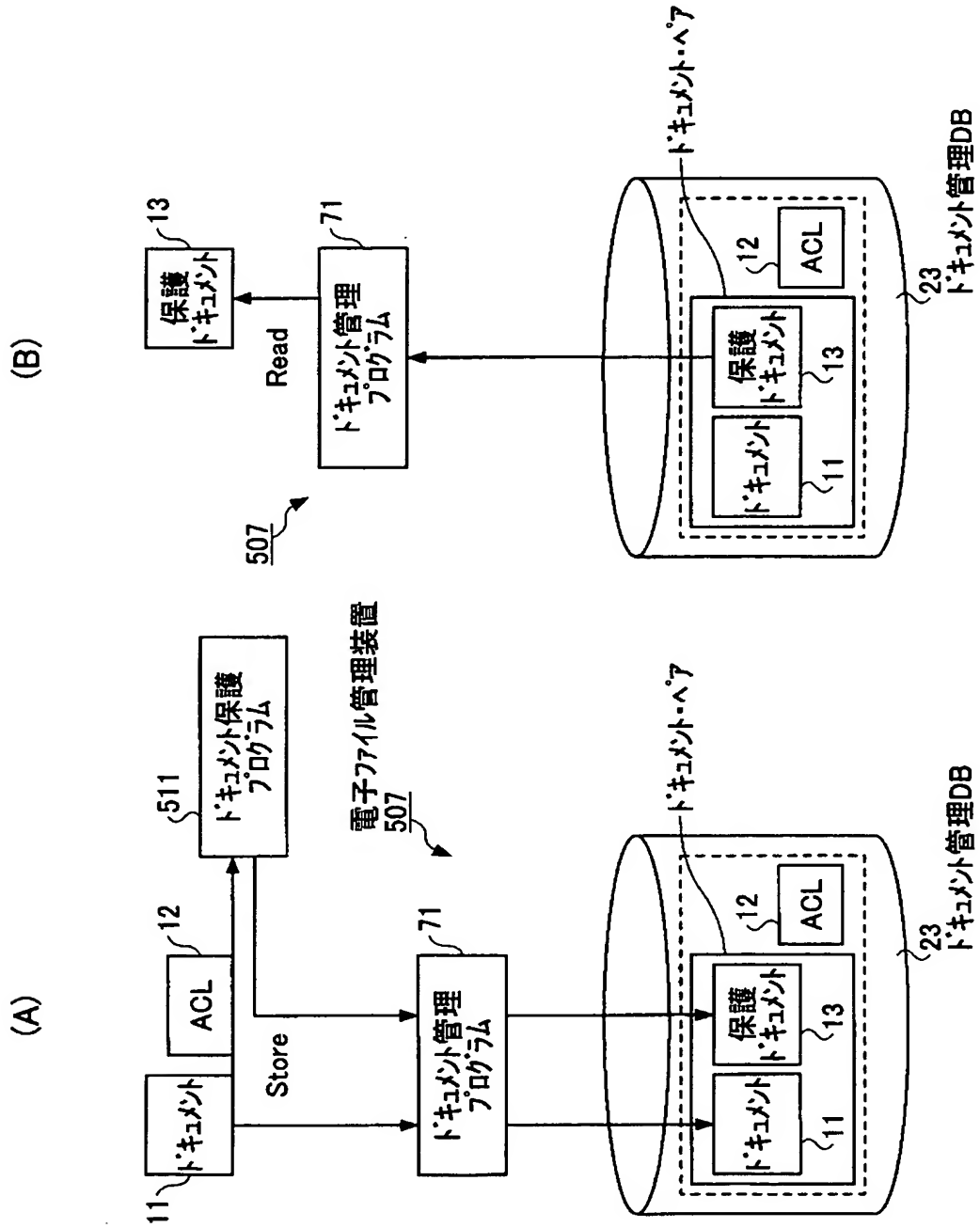
【図１５】

第3の実施形態に係るドキュメント管理プログラムによって実現される機能構成を示す図



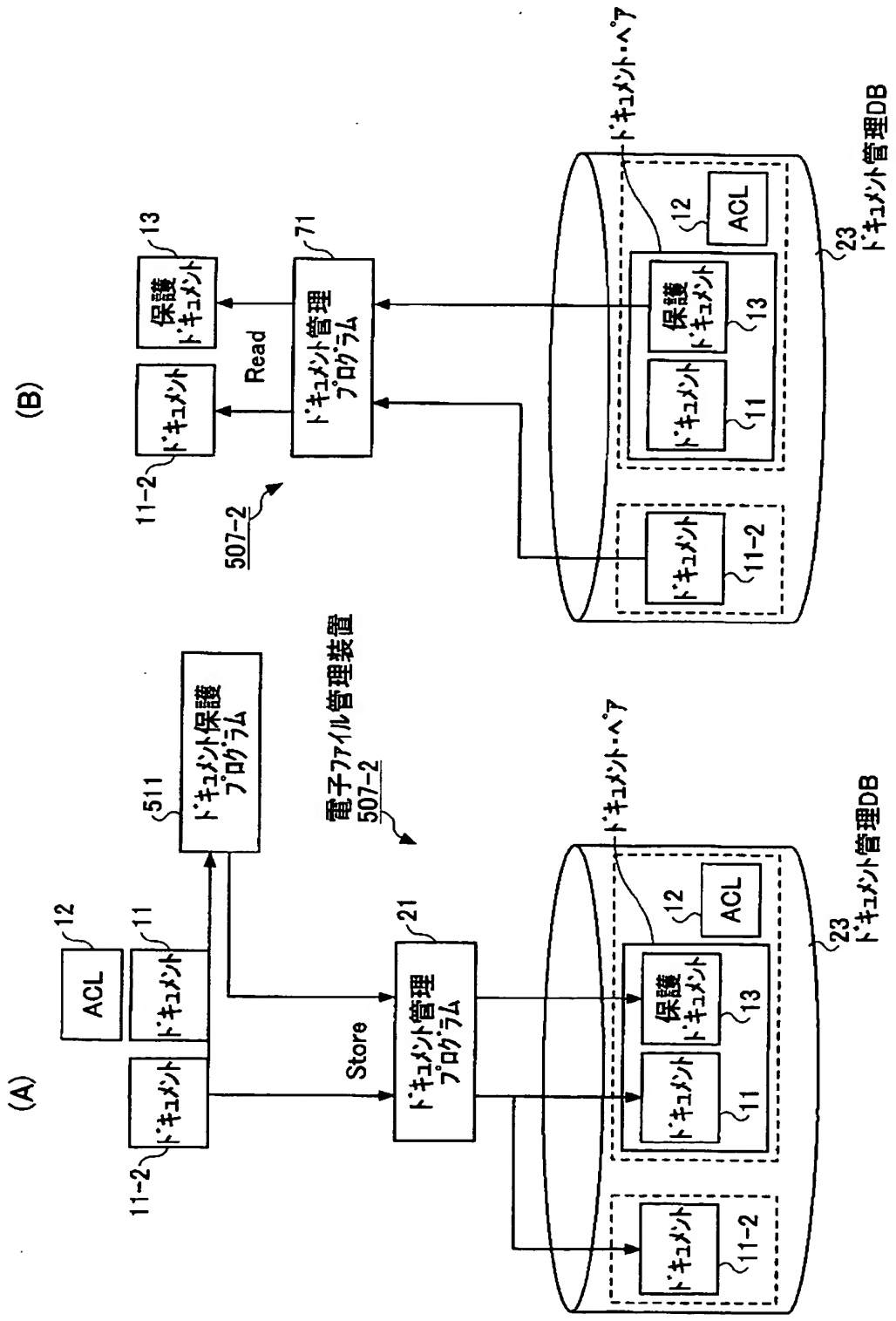
【図１６】

本発明の第4の実施形態に係る電子ファイル管理装置を示す図



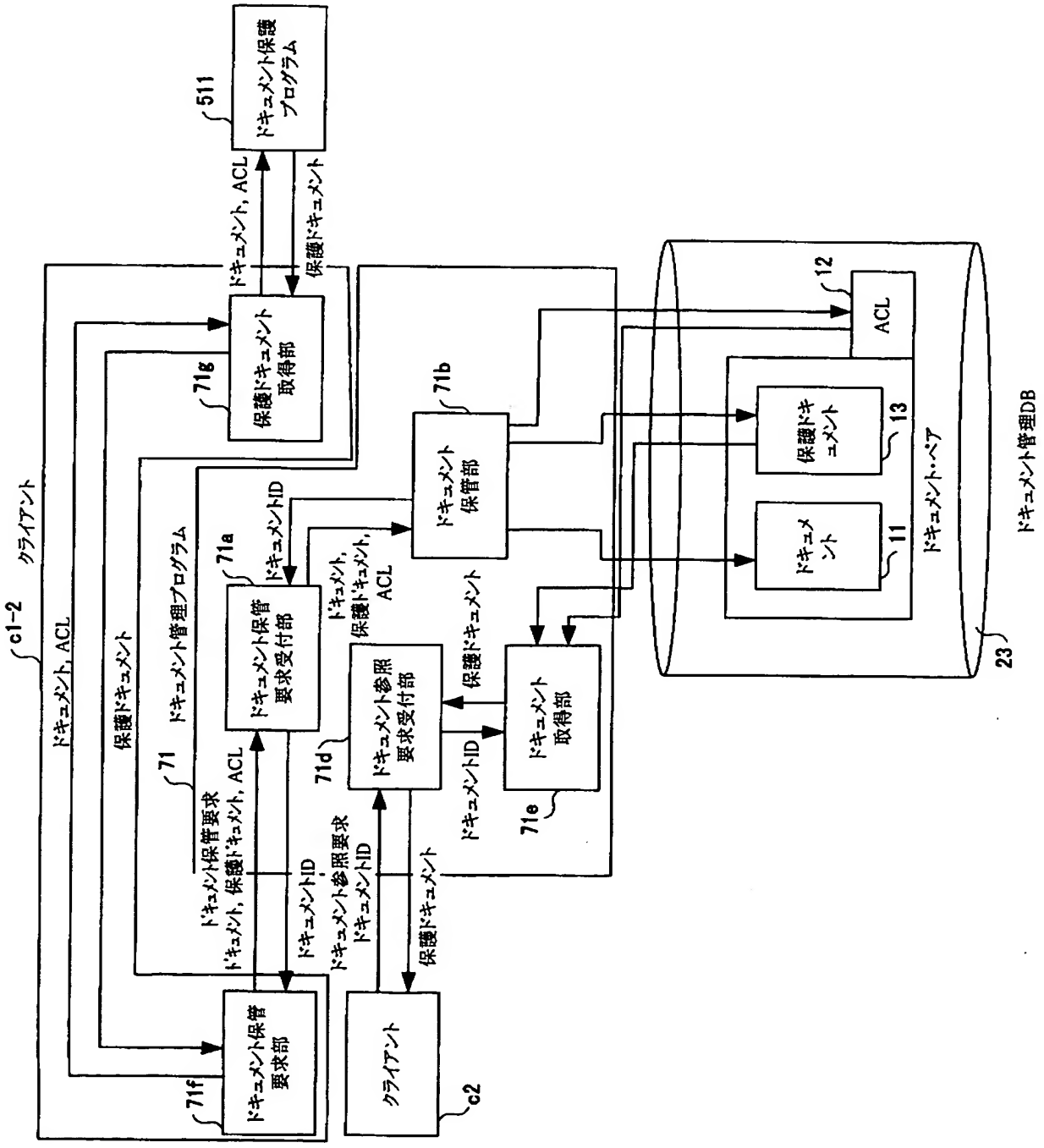
【図１７】

本発明の第4の実施形態に係る電子ファイル管理装置の他の例を示す図



【図１８】

第4の実施形態に係るドキュメント管理プログラムによって実現される機能構成を示す図



【図１９】

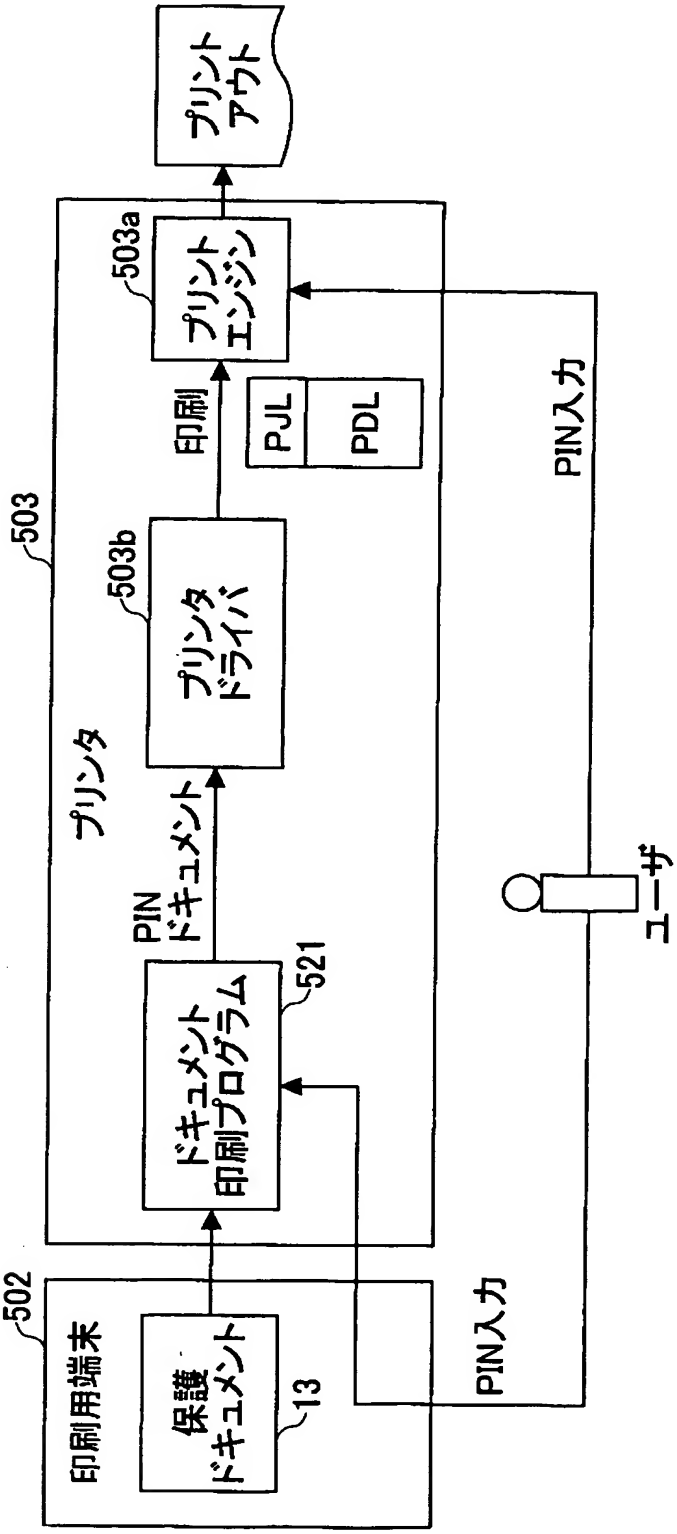
プリンタが備えるセキュリティ機能の例を示す図

プリントセキュリティ機能

スタンプ機能 (SLS)	マル秘などのマークをスタンプやウォーターマークとしてページ内の任意の場所に重ねて印刷する機能。スタンプに使用することができるのは「秘」や「CONFIDENTIAL」などの文字列やビットマップ画像である。
地紋印刷機能 (BDP)	複写機で複写されると特定のイメージが浮き上がるようにコントロールした地紋画像を原稿に重ね合わせて印刷する機能。上記のスタンプ機能でスタンプとして指定する画像を地紋画像にすることで実現する手法が一般的である。
機密印刷機能 (PAC)	印刷を指示する際にプリンタドライバにＰＩＮ（Personal Identification Number）を指定すると、印刷した本人がプリンタのところへ行き、プリンタのオペレーションパネルでそのＰＩＮを入力しなければプリントアウトされない機能。

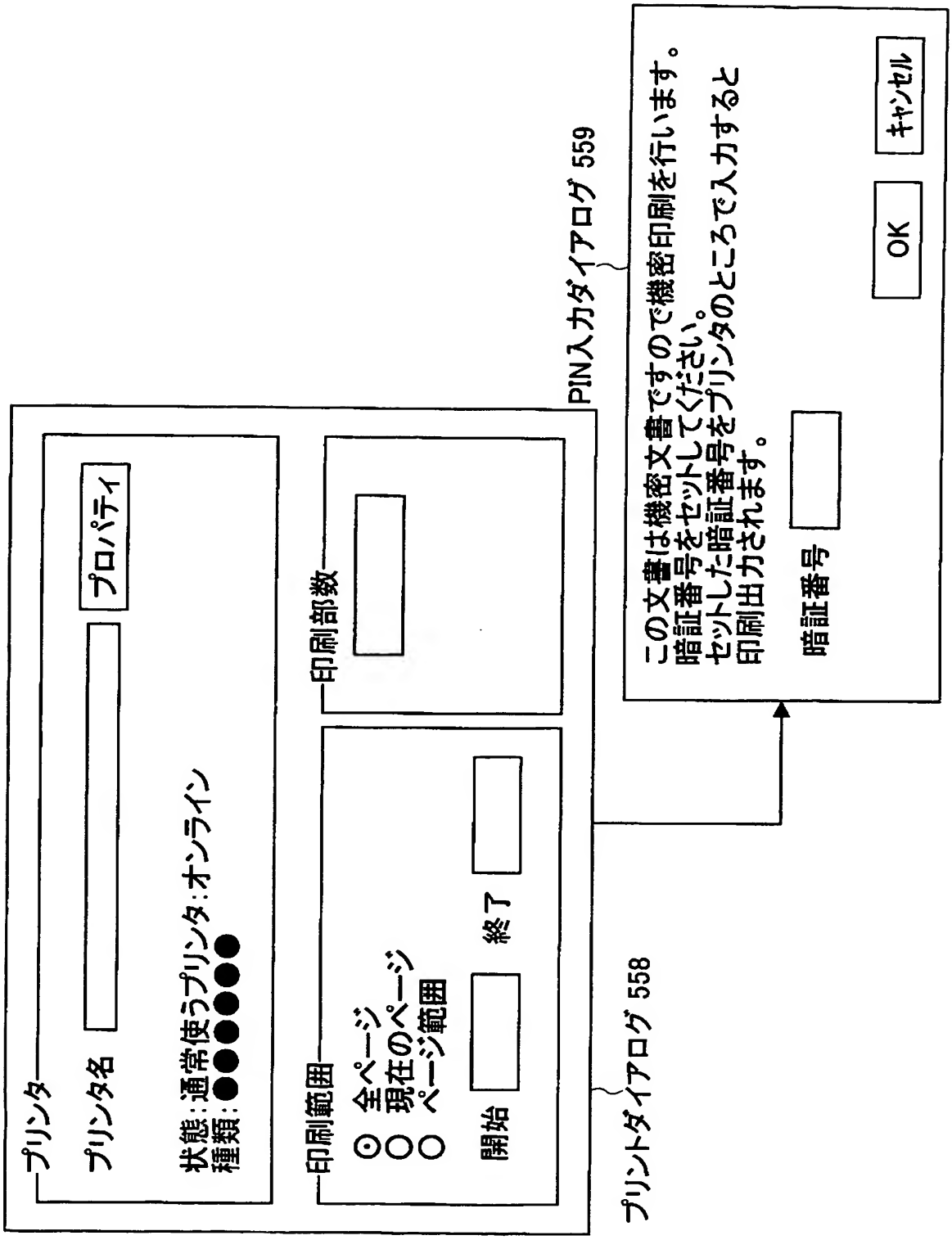
【図２０】

PACが設定されたドキュメントを印刷する際の処理を示す図



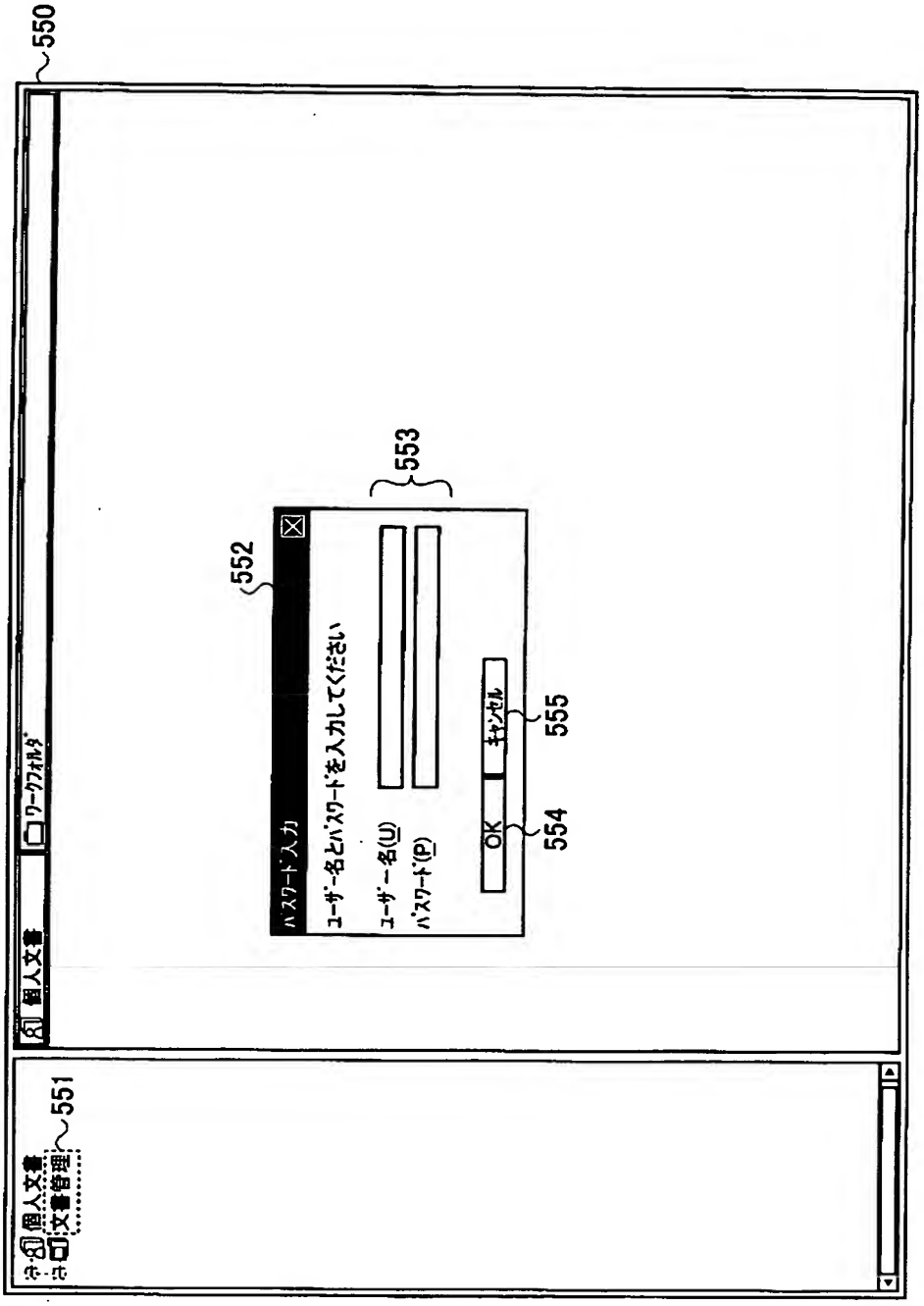
【図２１】

PIN入力のダイアログを示す図



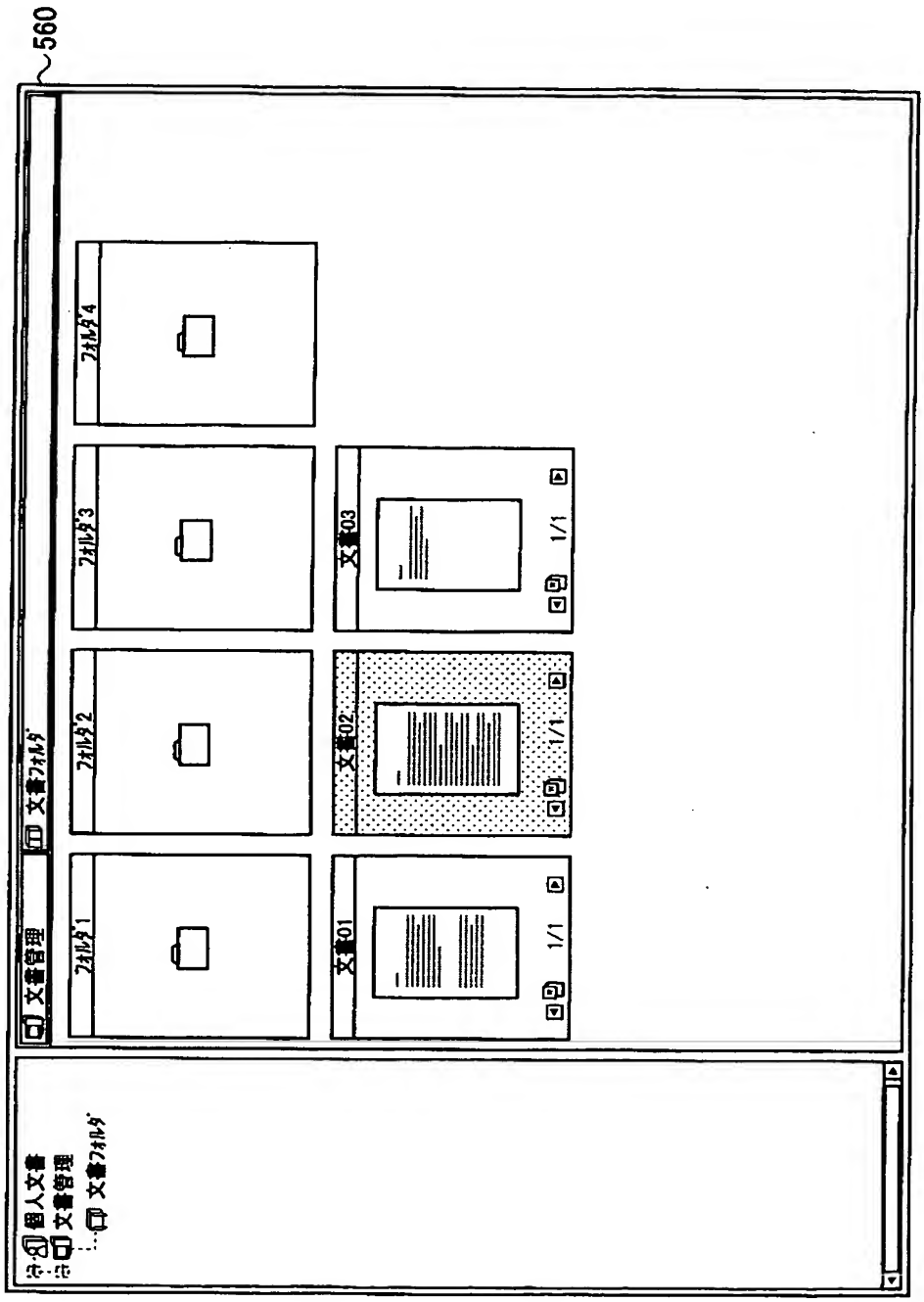
【図２２】

電子ファイル管理装置にアクセスした際に表示される画面例を示す図



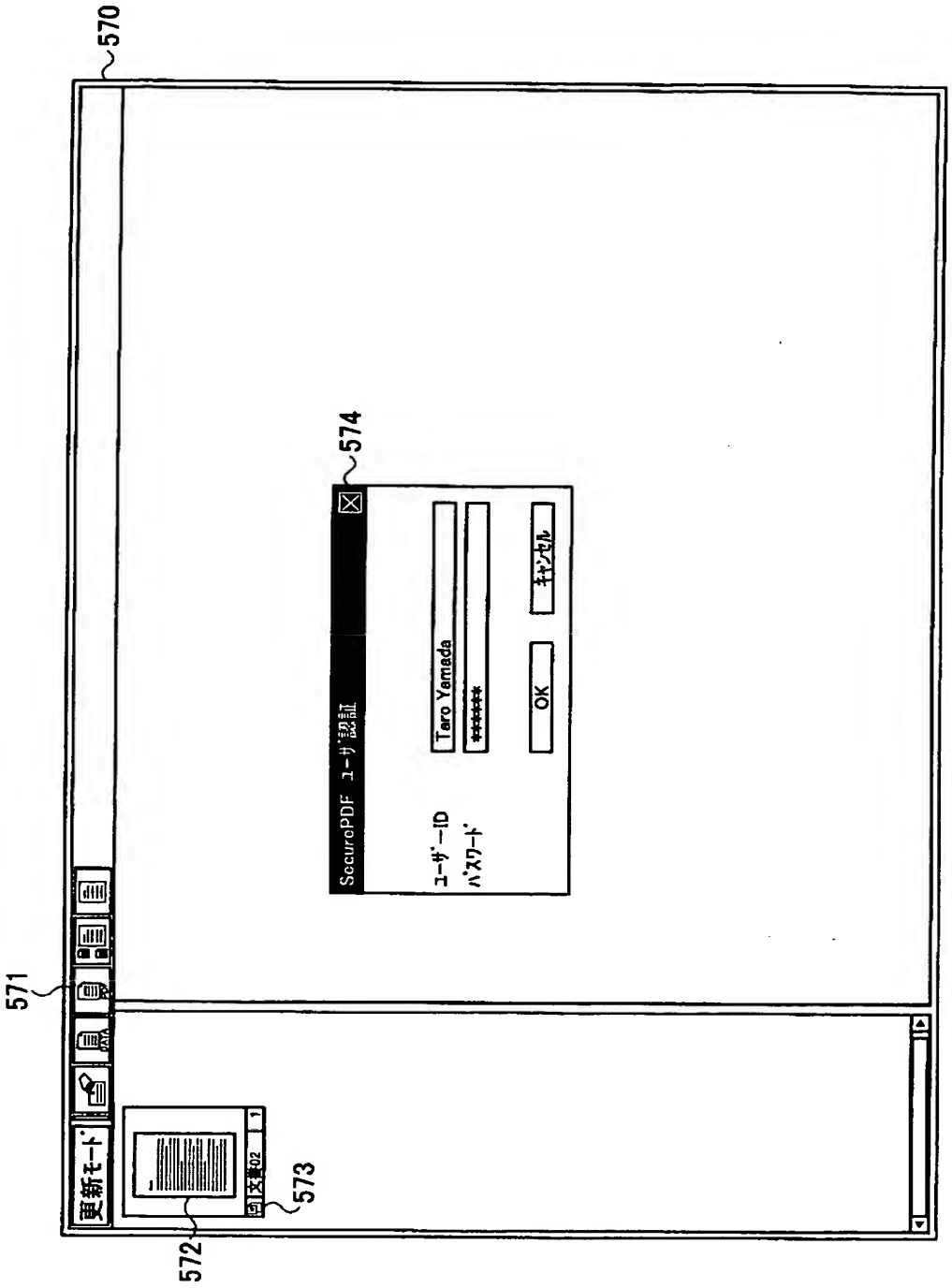
【図２３】

電子ファイル管理装置にて管理されるドキュメントの一覧を表示する画面例を示す図



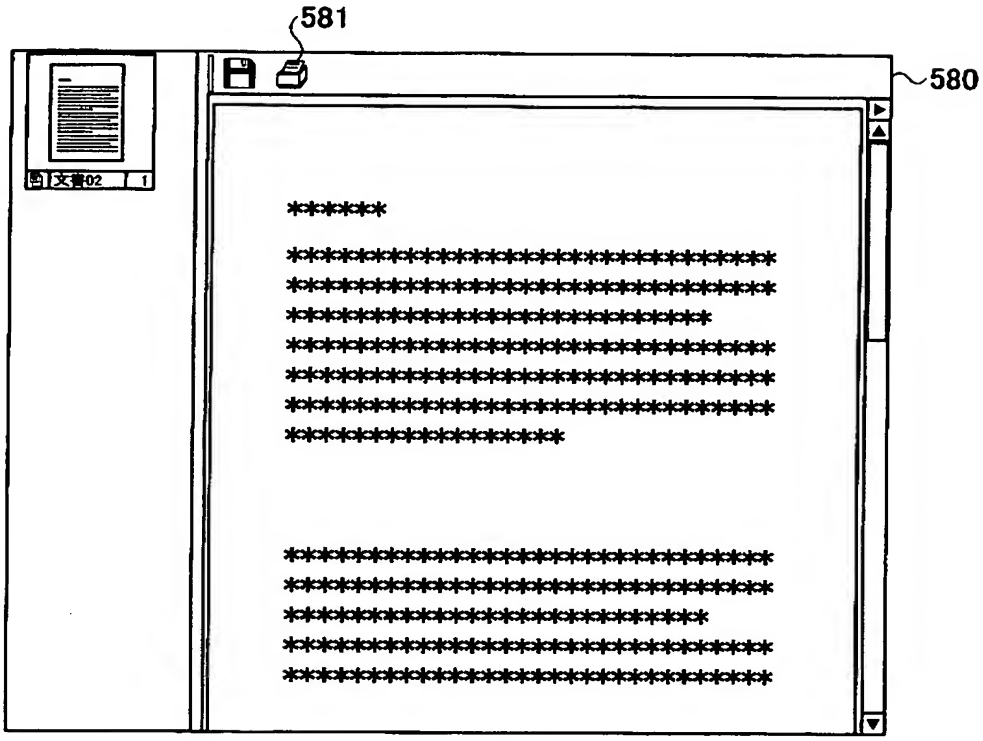
【図２４】

保護ドキュメントが提示されている画面例を示す図



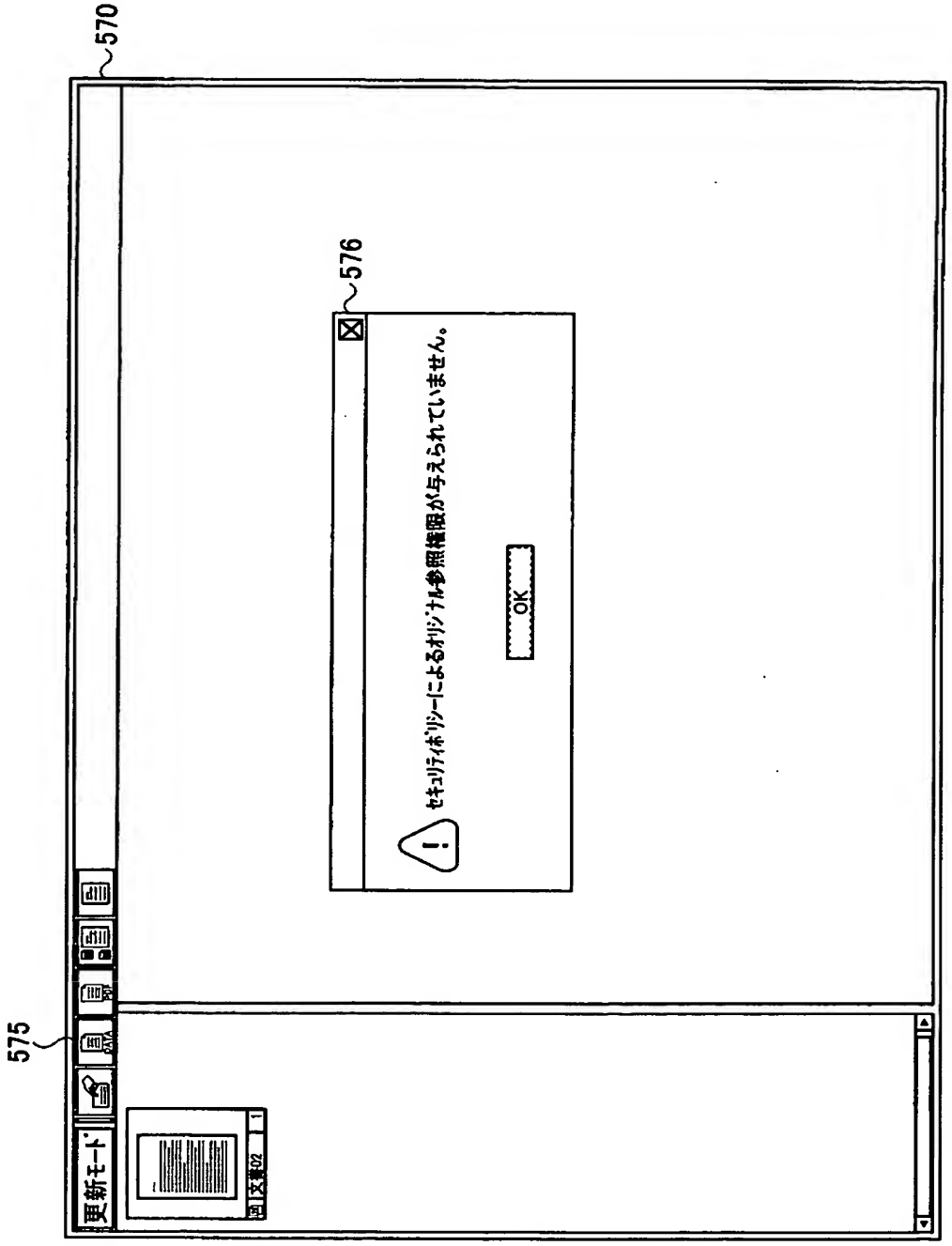
【図２５】

保護ドキュメントが開かれた状態を示す図



【図２６】

ユーザにオリジナル参照権限が与えられていない場合の画面例を示す図



【書類名】要約書
【要約】
【課題】　本発明の課題は、セキュリティを必要とする技術文書などの電子ファイルを管理し、アクセス権限に応じて該電子ファイルに対するアクセス制御を行う電子ファイル管理装置及びプログラム並びにファイルアクセス制御方法を提供することを目的とする。
【解決手段】　本発明の課題は、電子ファイルを格納する電子ファイル格納領域と、上記電子ファイルにアクセス権限情報を付加して上記電子ファイル格納領域に格納する電子ファイル管理手段と、上記電子ファイルへのアクセス要求に応じて、該電子ファイルを暗号化して保護した保護電子ファイルを出力する保護電子ファイル出力手段とを有する電子ファイル管理装置によって達成される。
【選択図】　図１

特願２００３－３１８４７５

出　願　人　履　歴　情　報

識別番号　　［０００００６７４７］

１．変更年月日　　２００２年　５月１７日
［変更理由］　　住所変更
住　所　　東京都大田区中馬込１丁目３番６号
氏　名　　株式会社リコー